MICRO FOCUS

Open Enterprise Server 2018 SP3

OES Remote Manager Administration Guide

July 2021

Legal Notices

© Copyright 2017 - 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 9

1 Overview of OES Remote Manager for Linux 11

1.1 Benefits of Using OES Remote Manager . . . 11
1.2 What's Next . . . 12

2 What's New or Changed in OES Remote Manager 15

2.1 What's New (OES 2018 SP3) . . . 15
2.2 What's New (OES 2018 SP2) . . . 15
2.3 What's New (OES 2018 SP1) . . . 15
2.4 What's New (OES 2018) . . . 15

3 Managing a Virtualized Linux Server with OES Remote Manager 17

4 Installing OES Remote Manager for Linux 19

4.1 Installing OES Remote Manager During the Initial Server Installation . . . 19
4.2 Installing OES Remote Manager After the Initial Server Installation . . . 19

5 Accessing OES Remote Manager for Linux 21

5.1 System Requirements . . . 21
5.2 Accessing OES Remote Manager . . . 22
5.3 Starting or Stopping HTTPSTKD . . . 23
5.4 Understanding the Layout of OES Remote Manager . . . 24
5.4.1 Header Frame . . . 26
5.4.2 Overall Health Indicator . . . 26
5.4.3 Navigation Frame . . . 27
5.4.4 Program Plug-Ins in the Navigation Frame . . . 28
5.4.5 Main Content Frame . . . 28
5.4.6 Online Help . . . 28
5.5 Accessing Configuration Options . . . 29
5.6 Accessing Online Help . . . 29
5.7 Accessing Micro Focus Web Pages . . . 29

6 Changing the HTTPSTKD Configuration 31

6.1 Accessing and Editing the HTTPSTKD Configuration File . . . 33
6.2 Accessing and Editing the HTTPSTKD PAM Configuration File . . . 34
6.3 Restarting the HTTPSTKD Daemon . . . 35
6.4 Viewing the HTTP Logs . . . 35
6.5 Viewing and Creating Certificates for OES Remote Manager . . . 36
6.6 Extending the eDirectory Schema for OES Remote Manager Group Operations . . . 37

7 Diagnosing Problems Using Ganglia and Nagios 39

7.1 Monitoring Server Health . . . 40
7.1.1 Viewing the Overall Server Health Status . . . 40
7.2 Configuring Ganglia . . . 40
7.2.1 Ganglia Requirements . . . 41
7.2.2 Configuring Ganglia gmond in Multicast Mode or Unicast Mode . . . 42
7.3 Stopping and Starting Ganglia gmond and gmetad . . . 44
7.4 Monitoring Server Health with Ganglia . . . 44
7.5 Configuring Nagios . . . 47
7.5.1 Configuring Nagios Authenticated Users and Contacts . . . 47
7.5.2 Configuring Nagios Monitoring . . . 51
7.5.3 Accessing the Nagios Website . . . 53
7.5.4 Using Nagios Plug-Ins . . . 54
7.5.5 Using Object Configuration Files . . . 54
7.5.6 Additional Information . . . 54
7.6 Monitoring Service Health with Nagios . . . 55
7.7 Restarting Nagios . . . 55
7.8 Managing Nagios Users . . . 56
7.8.1 Creating or Re-Creating a Nagios User . . . 56
7.8.2 Setting Passwords for Nagios Users . . . 57
7.8.3 Deleting a Nagios User . . . 57
7.8.4 Configuring Nagios Contacts and Notification Methods for Them . . . 57
7.8.5 Configuring Nagios CGI Authorization for Contacts . . . 58
7.9 Modifying the Nagios Notification Methods for Contacts . . . 58
7.10 Configuring Nagios Logging . . . 59
7.11 Viewing the PIDs or Monitoring the Health of Processes . . . 61
7.12 Monitoring or Killing an Individual Process . . . 62
7.13 Troubleshooting a Suspect or Bad Health Status . . . 63

8 Viewing File Systems 65

8.1 Viewing Mounted Devices and Performing Actions on Them . . . 66
8.2 Browsing File Systems and Performing Actions on Them . . . 67
8.2.1 Viewing or Changing File or Directory Attributes . . . 69
8.2.2 Viewing Details about Directories and Performing Actions on Them . . . 69
8.2.3 Uploading a File to the Server . . . 70
8.2.4 Downloading a File from the Server to a Local Workstation . . . 70
8.2.5 Searching for Text in Files . . . 71
8.2.6 Viewing the Details of a File and Performing Specific Actions . . . 71
8.2.7 Viewing Individual Files . . . 72
8.3 Viewing Partition Information . . . 72

9 Managing Linux 73

9.1 Accessing VNC Consoles . . . 73
9.2 Viewing Kernel Modules . . . 75
9.3 Shutting Down and Restarting the Host . . . 76
9.4 Managing Packages . . . 77
9.5 Managing Processes . . . 79
9.6 Scheduling cron Jobs to Run on the Server . . . 80

10 Managing Hardware **83**

10.1 Viewing Processors . . . 83
10.2 Viewing Interrupt Information . . . 84
10.3 Viewing I/O Memory Information . . . 85
10.4 Viewing I/O Port Information . . . 86
10.5 Viewing SMBIOS Information . . . 87

11 Using Group Operations **89**

11.1 Building and Configuring a Monitoring Group . . . 90
11.2 Saving a Group . . . 94
11.2.1 Saving the Group to the Local Server . . . 94
11.2.2 Saving the Group and Associating It with an eDirectory Object . . . 95
11.3 Accessing an Existing Group . . . 95
11.4 Changing an Existing Group . . . 95
11.5 Deleting an Existing Group . . . 96
11.6 Generating and Viewing Server Reports . . . 96
11.6.1 Compare Server Up Time Report . . . 96
11.7 Viewing Monitored Items . . . 97
11.8 Viewing Group Monitoring Types . . . 98
11.9 Defining or Editing Group Monitoring Types . . . 98
11.10 Discovering Items on the Network to Monitor . . . 99

12 Managing NCP Services **103**

12.1 Quick Reference for the NCP Server Plug-In for OES Remote Manager for Linux . . . 105
12.1.1 NCP Volumes (NCP Shares) . . . 105
12.1.2 NCP Server Parameters . . . 106
12.1.3 NCP Server Connections . . . 106
12.1.4 NCP Trustee Reports . . . 107
12.1.5 NCP Logs and Audit Logs . . . 107
12.1.6 NCP Server Statistics . . . 108
12.1.7 NCP Server Diagnostics . . . 108
12.1.8 Dynamic Storage Technology . . . 109
12.2 Browsing NSS Volumes and Performing Actions on Them . . . 110
12.2.1 Viewing Information about an NSS Volume . . . 111
12.2.2 Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It . . . 113
12.2.3 Viewing the Linux POSIX Details of a File and Performing Specific Actions on It . . . 113
12.2.4 Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files . . . 114
12.2.5 Salvaging and Purging Deleted Files on an NSS Volume . . . 118
12.2.6 Purging a Deleted NSS Volume . . . 118
12.2.7 Viewing Open File Information for an NSS Volume . . . 119
12.3 Generating Inventories for Directories or NCP Volumes . . . 119
12.3.1 Generating a File Inventory Report . . . 120
12.3.2 Generating an NCP Volume Inventory Report . . . 122
12.3.3 Viewing a Saved NCP Inventory Report . . . 124
12.4 Generating a Custom Inventory Report from a File Inventory Report . . . 125
12.5 Performing Actions on Files from Custom Reports . . . 126
12.5.1 Moving Selected Files . . . 126
12.5.2 Copying Selected Files . . . 127

12.5.3 Deleting Selected Files 127
12.5.4 Opening or Downloading a File 127
12.5.5 Managing Individual Files. 127
12.6 Generating and Viewing NCP Trustee Reports for NSS Volumes 128
12.6.1 Generating an NCP Trustee Report 128
12.6.2 Viewing a Saved NCP Trustee Report 129

13 Managing Dynamic Storage Technology Options 131

14 Managing CIFS Services 135

14.1 Managing CIFS Connections 135
14.2 Viewing Log Information 136
14.3 Managing Open Files 137

15 Managing AFP Services 139

15.1 Managing AFP Connections 140
15.2 Viewing Log Information 141
15.3 Managing Open Files 141

16 Tasks Quick Reference 143

17 Troubleshooting OES Remote Manager 147

17.1 Daemon httpstkd Is Unable to Start 147
17.2 Error while loading shared libraries: libldapx.so.0 147
17.3 Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2018
or Later 148
17.4 Ganglia Statistical Graphics Are Not Displayed in the Web Browser 149
17.4.1 Firefox 149
17.4.2 Internet Explorer. 150
17.4.3 Chrome 150

18 Security Considerations 151

18.1 Security Features 151
18.2 Security Characteristics 153
18.3 Security Configuration. 154
18.4 Nagios Security Configuration 156

A HTTPSTKD Configuration File Options 157

A.1 Address and Port Commands 157
A.2 Disable Auto LUM Command 158
A.3 Filtering Commands. 160
A.4 HttpOnly Command. 161
A.5 InventoryResolveNonLumOwnerName Command. 162
A.6 Language Commands 162
A.7 Load Command 164

A.8 SSL Key Cipher Strength Command 165
A.9 Supervisor Only Command 165

B OES Remote Manager Packages 167

About This Guide

This guide describes how to access and use OES Remote Manager on a host that is running Open Enterprise Server (OES) 2018 SP3. This guide includes the following information:

- Chapter 1, “Overview of OES Remote Manager for Linux,” on page 11
- Chapter 2, “What’s New or Changed in OES Remote Manager,” on page 15
- Chapter 3, “Managing a Virtualized Linux Server with OES Remote Manager,” on page 17
- Chapter 4, “Installing OES Remote Manager for Linux,” on page 19
- Chapter 5, “Accessing OES Remote Manager for Linux,” on page 21
- Chapter 6, “Changing the HTTPSTKD Configuration,” on page 31
- Chapter 7, “Diagnosing Problems Using Ganglia and Nagios,” on page 39
- Chapter 8, “Viewing File Systems,” on page 65
- Chapter 9, “Managing Linux,” on page 73
- Chapter 10, “Managing Hardware,” on page 83
- Chapter 11, “Using Group Operations,” on page 89
- Chapter 12, “Managing NCP Services,” on page 103
- Chapter 13, “Managing Dynamic Storage Technology Options,” on page 131
- Chapter 14, “Managing CIFS Services,” on page 135
- Chapter 15, “Managing AFP Services,” on page 139
- Chapter 16, “Tasks Quick Reference,” on page 143
- Chapter 17, “Troubleshooting OES Remote Manager,” on page 147
- Chapter 18, “Security Considerations,” on page 151
- Appendix A, “HTTPSTKD Configuration File Options,” on page 157
- Appendix B, “OES Remote Manager Packages,” on page 167

Audience

This guide is intended for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to Micro Focus Documentation Feedback (https://www.microfocus.com/documentation/open-enterprise-server/2018-SP3/) and enter your comments there.

Documentation Updates

For the most recent version of the *OES Remote Manager Administration Guide*, visit the OES 2018 SP3 documentation website (https://www.microfocus.com/documentation/open-enterprise-server/2018-SP3/).

Additional Documentation

For information about other OES services and file systems, see the OES 2018 SP3 documentation website (https://www.microfocus.com/documentation/open-enterprise-server/2018-SP3/).

1 Overview of OES Remote Manager for Linux

OES Remote Manager (NRM) for Linux is a browser-based utility that you can use to manage one or more Linux servers from a remote location.

You can use OES Remote Manager to monitor your server's health, change the configuration of your server, or perform diagnostic and debugging tasks.

The advantages of using OES Remote Manager for server management are that:

- It does not require a special client.
- It provides a graphical interface that makes interpreting diagnostic information much more comprehensive and easier to manage.
- It provides added functionality that is not available in the other management utilities.

This section explains the following:

- Section 1.1, "Benefits of Using OES Remote Manager," on page 11
- Section 1.2, "What's Next," on page 12

1.1 Benefits of Using OES Remote Manager

Organizations usually don't have a technician physically located at the server when it needs attention. Servers are frequently placed in remote or distributed locations and, in the case of service providers, at many different companies. The ability to centrally monitor, diagnose, and repair (or preventively avoid) server problems is a significant advantage. It is also a major benefit to be able to provide technical service from any location—any point in the world—across the Internet.

OES Remote Manager provides IT staff and service providers the ability to monitor and control a complete selection of server controls and functions through a standard web browser.

The management power and flexibility now available simplifies network administration and allows fewer staff to effectively manage more resources. OES Remote Manager lets you do the following:

- Securely access and manage a Linux server from any location. With proper login credentials and Internet access, administrators can control servers from any location.
- Group servers for collective management, allowing you to manage multiple servers through the same interface and application.
- Quickly locate and assess problems. An intuitive graphical user interface provides a control dashboard with indicators for server health and status.
- Manage servers comprehensively. OES Remote Manager provides control for viewing or managing Linux servers, directories, processes, and hardware.

While using OES Remote Manager, you can perform the following major tasks:

- Monitor and manage your server's health
  - Monitor the health status of one or more servers
  - Build a group of servers and items to be monitored together
  - Access server and configuration logs
- Configure your server
  - View information about all hardware adapters, hardware resources, and processor data
  - Upload and replace files
  - Monitor memory resources
  - Access files
  - Shut down or reset a server
- Troubleshoot server problems
  - Find high memory users
  - Monitor server processes

1.2 What's Next

Now that you have learned some of the benefits of using OES Remote Manager, use the information in Table 1-1 and Table 1-2 to help you access and use it.

Table 1-1 *Information about OES Remote Manager*

For Information About	See
Accessing and understanding the layout of OES Remote Manager	Chapter 5, "Accessing OES Remote Manager for Linux," on page 21
Managing a virtualized OES server with OES Remote Manager.	Chapter 3, "Managing a Virtualized Linux Server with OES Remote Manager," on page 17
Installing OES Remote Manager for Linux	Chapter 4, "Installing OES Remote Manager for Linux," on page 19
Changing the configuration of OES Remote Manager	Chapter 6, "Changing the HTTPSTKD Configuration," on page 31
Using OES Remote Manager to monitor and manage your OES servers	◆ Chapter 7, "Diagnosing Problems Using Ganglia and Nagios," on page 39 ◆ Chapter 8, "Viewing File Systems," on page 65 ◆ Chapter 9, "Managing Linux," on page 73 ◆ Chapter 10, "Managing Hardware," on page 83 ◆ Chapter 11, "Using Group Operations," on page 89
Things to consider for setting up your system in a secure environment.	Chapter 18, "Security Considerations," on page 151

Table 1-2 *Information about Plug-Ins to OES Remote Manager*

For Information About	See
Dynamic Storage Technology	◆ Chapter 12, “Managing NCP Services,” on page 103 ◆ *OES 2018 SP3: Dynamic Storage Technology Administration Guide*
NCP Server	◆ Chapter 12, “Managing NCP Services,” on page 103 ◆ *OES 2018 SP3: NCP Server for Linux Administration Guide*
OES AFP (in OES 2015 and later)	◆ Chapter 15, “Managing AFP Services,” on page 139 ◆ *OES 2018 SP3: OES AFP for Linux Administration Guide*
OES CIFS (in OES 2015 and later)	◆ Chapter 14, “Managing CIFS Services,” on page 135 ◆ *OES 2018 SP3: OES CIFS for Linux Administration Guide*

2 What's New or Changed in OES Remote Manager

This section describes the changes made to OES Remote Manager since the Open Enterprise Server (OES) 2018 release.

- Section 2.1, "What's New (OES 2018 SP3)," on page 15
- Section 2.2, "What's New (OES 2018 SP2)," on page 15
- Section 2.3, "What's New (OES 2018 SP1)," on page 15
- Section 2.4, "What's New (OES 2018)," on page 15

2.1 What's New (OES 2018 SP3)

Beginning with OES 2018 SP3, OES Remote Manager uses encryption for enhanced security.

2.2 What's New (OES 2018 SP2)

OES Remote Manager in OES 2018 SP2 has been modified for bug fixes. There are no new features or enhancements in OES 2018 SP2.

2.3 What's New (OES 2018 SP1)

OES Remote Manager in OES 2018 SP1 has been modified for bug fixes. There are no new features or enhancements in OES 2018 SP1.

2.4 What's New (OES 2018)

In addition to bug fixes, OES Remote Manager (NRM) user interface has been refreshed to provide a new and modern look.

3 Managing a Virtualized Linux Server with OES Remote Manager

Using OES Remote Manager for Linux to access and manage a virtualized Open Enterprise Server (OES) 11 or later server is the same in every way as accessing and managing a physical OES 11 or later server. It requires no special configuration or other changes.

To get started with Xen virtualization and KVM virtualization, see the *Virtualization Guide* (https://www.suse.com/documentation/sles-12/book_virt/data/book_virt.html).

For information about setting up virtualized OES, see "Installing, Upgrading, or Updating OES on a VM" in the *OES 2018 SP3: Installation Guide*.

To get started with third-party virtualization platforms, such as Hyper-V from Microsoft and the different VMware product offerings, refer to the documentation for the product you are using.

4 Installing OES Remote Manager for Linux

OES Remote Manager is installed as a Open Enterprise Server (OES) service pattern in the YaST Install. This section contains the following information:

- Section 4.1, “Installing OES Remote Manager During the Initial Server Installation,” on page 19
- Section 4.2, “Installing OES Remote Manager After the Initial Server Installation,” on page 19

4.1 Installing OES Remote Manager During the Initial Server Installation

To install OES Remote Manager during the OES installation or while adding OES on an existing server, select the OES Remote Manager (NRM) pattern to install OES Remote Manager.

It does not require any additional configuration during the installation and does not display on the Installation Settings page. For information about changing the configuration after the installation is complete, see Chapter 6, “Changing the HTTPSTKD Configuration,” on page 31.

For a list of RPMs that it installs, see Appendix B, “OES Remote Manager Packages,” on page 167.

4.2 Installing OES Remote Manager After the Initial Server Installation

If you did not install OES Remote Manager when you first installed OES, do the following to install and configure NRM:

1. Open YaST.
2. Click **Open Enterprise Server** > **OES Install and Configuration**.
3. Select the OES Remote Manager (NRM) pattern.

   Selecting this pattern automatically selects the OES Linux User Management (LUM) and OES Backup/Storage Management Services (SMS) patterns.
4. If you have only installed NRM, then you can log in to NRM only as user `root` or a local Linux user. If you log in as a local Linux user, you can see only the information that the user you log in as has rights to view.
5. Click **Accept**.
6. If necessary, complete any required information for other services selected on the Micro Focus Open Enterprise Server Configuration summary page. When all the settings on the Micro Focus Open Enterprise Server Configuration summary page are set as desired, click **Next**.

   The necessary files are installed and configuration of the services are completed.

No additional configuration during the installation for NRM is required. For information about changing the configuration after the installation is complete, see Chapter 6, “Changing the HTTPSTKD Configuration,” on page 31.

For a list of RPMs that it installs, see Appendix B, “OES Remote Manager Packages,” on page 167.

5 Accessing OES Remote Manager for Linux

This section includes information about the following:

- Section 5.1, “System Requirements,” on page 21
- Section 5.2, “Accessing OES Remote Manager,” on page 22
- Section 5.3, “Starting or Stopping HTTPSTKD,” on page 23
- Section 5.4, “Understanding the Layout of OES Remote Manager,” on page 24
- Section 5.5, “Accessing Configuration Options,” on page 29
- Section 5.6, “Accessing Online Help,” on page 29
- Section 5.7, “Accessing Micro Focus Web Pages,” on page 29

5.1 System Requirements

- ❒ Supported web browsers:
  - Mozilla Firefox 12 or later
  - Microsoft Internet Explorer (IE) 8 and 9. IE 10 and 11 is supported for Windows 7 and 8 clients in the desktop view only.
  - Apple Safari 5 and Safari 6.0 (for Mac OS X Mountain Lion (version 10.8) clients only)
  - Google Chrome 21 or later
  - KDE Konqueror 4 or later, with limited functionality
- ❒ Certificate handling requires SSL 2.0 or later or TLS 1.0 or later to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0 or the latest TLS if it is available.
- ❒ The HTTPSTKD package must be loaded and running on the server.

  For information about starting or restarting the `httpstkd` daemon, see Section 5.3, “Starting or Stopping HTTPSTKD,” on page 23.

  This package is selected for installation by the OES Remote Manager pattern. The OES Remote Manager (NRM) pattern is selected for installation when you install any of the OES Services patterns on Linux unless you deselect it.

  For information about installing OES Remote Manager, see Chapter 4, “Installing OES Remote Manager for Linux,” on page 19.

  For package details, see “OES Remote Manager Packages” on page 167.

5.2 Accessing OES Remote Manager

You typically log in as the Linux `root` user to manage all functions in OES Remote Manager. The `root` user can access OES Remote Manager even when eDirectory is not available.

Some functions support access by administrator users who are eDirectory users and who are also enabled for Linux with Linux User Management (LUM-enabled). If LUM is enabled in your tree and it is installed and configured on the server, you can log in to OES Remote Manager using your eDirectory credentials. For instructions on enabling Linux, see "Setting Up Linux Computers to Use eDirectory Authentication" in the *OES 2018 SP3: Linux User Management Administration Guide*.

If you log in as a local Linux user or as a non-Admin LUM-enabled eDirectory user, you can see only the information that the user has rights to view. Typically, access is restricted to a view of the Linux file systems where the user has file system access rights.

There are two specific things to remember when logging in to OES Remote Manager as a LUM-enabled eDirectory user:

- If eDirectory and LUM are installed on the local server, the eDirectory user Admin can log in to OES Remote Manager using its fully distinguished name (admin.context) because this user is enabled for Linux User Management by default in this case.

  In order for a user to log in to OES Remote Manager as user Admin or equivalent, you must configure either of the following permissions for the Admin user:

  - The Admin user must be associated to the group that has the Supervisor right for the Entry Rights property for the UNIX Workstation object.
  - The Admin user must have the Supervisor right for the Entry Rights to the NCP object that represents the Linux server in the eDirectory tree.

  IMPORTANT: With either of these permissions, the eDirectory user is granted limited `root` user privileges when logged in to the server. The user can modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying.

- In order for non-Admin users to log in using eDirectory credentials, they must be users enabled for Linux User Management.

  Users who are enabled for Linux User Management have a Linux Profile tab on their Modify User page in iManager. They also have an eDirectory object that is associated with the UNIX Workstation object that represents the Linux server.

  You can use iManager or the LUM command line utility `namuseradd` to enable users for Linux User Management. For instructions, see "Overview" in the *OES 2018 SP3: Linux User Management Administration Guide*.

The Admin user has limited file system rights equivalent to `root`. The user can modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. For a list of these files, see Section 18.1, "Security Features," on page 151. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.

To access to OES Remote Manager:

1. Open a web browser.
2. Point the browser to the URL of the server you want to manage by entering the following in the Address (URL) field:

   `http://server_ip_address:8008`

   or

   `https://server_ip_address:8009`

   If you specify HTTP and port 8008, you are automatically re-directed to use secure HTTP (HTTPS) and port 8009.

   For example, either of the following URLs take you to a secure SSL login page for OES Remote Manager on the specified server:

   `http://172.16.123.11:8008`

   `https://172.16.123.11:8009`
3. Accept the SSL certificate.

   Certificate handling requires SSL 2.0 or later, or TLS 1.0 or later, to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0 or the latest TLS if it is available.
4. When the login dialog box appears, provide the required **Username** and **Password** credentials.

   Typically, you log in with the Linux `root` user name and password.
5. Use the links in OES Remote Manager to view, configure, and manage the server.

   For information about navigating in OES Remote Manager, see Section 5.4, “Understanding the Layout of OES Remote Manager,” on page 24.
6. After your session for OES Remote Manager is complete, click **Logout** at the top-right corner to log out, then close the web browser.

   After you log in, your session for OES Remote Manager remains open until you log out or close your web browser. There is no automatic time-out period that triggers a logout. For security reasons, you should also close the browser windows at that workstation after you log out.

5.3 Starting or Stopping HTTPSTKD

When you install and configure the OES Remote Manager pattern on Open Enterprise Server (OES) server, NRM is started by default.

A script for starting and stopping the NRM/Linux components is in `/usr/lib/systemd/system/novell-httpstkd.service`. Enter the following commands at a console shell prompt to perform the desired action:

Table 5-1 *Commands for Starting, Stopping, or Checking the Status of NRM*

Task	Command

To see whether the module is running	`rcnovell-httpstkd status`
	or
	`systemctl status novell-httpstkd.service`

To restart HTTPSTKD	`rcnovell-httpstkd restart`
	or
	`systemctl restart novell-httpstkd.service`

To start HTTPSTKD	`rcnovell-httpstkd start`
	or
	`systemctl start novell-httpstkd.service`

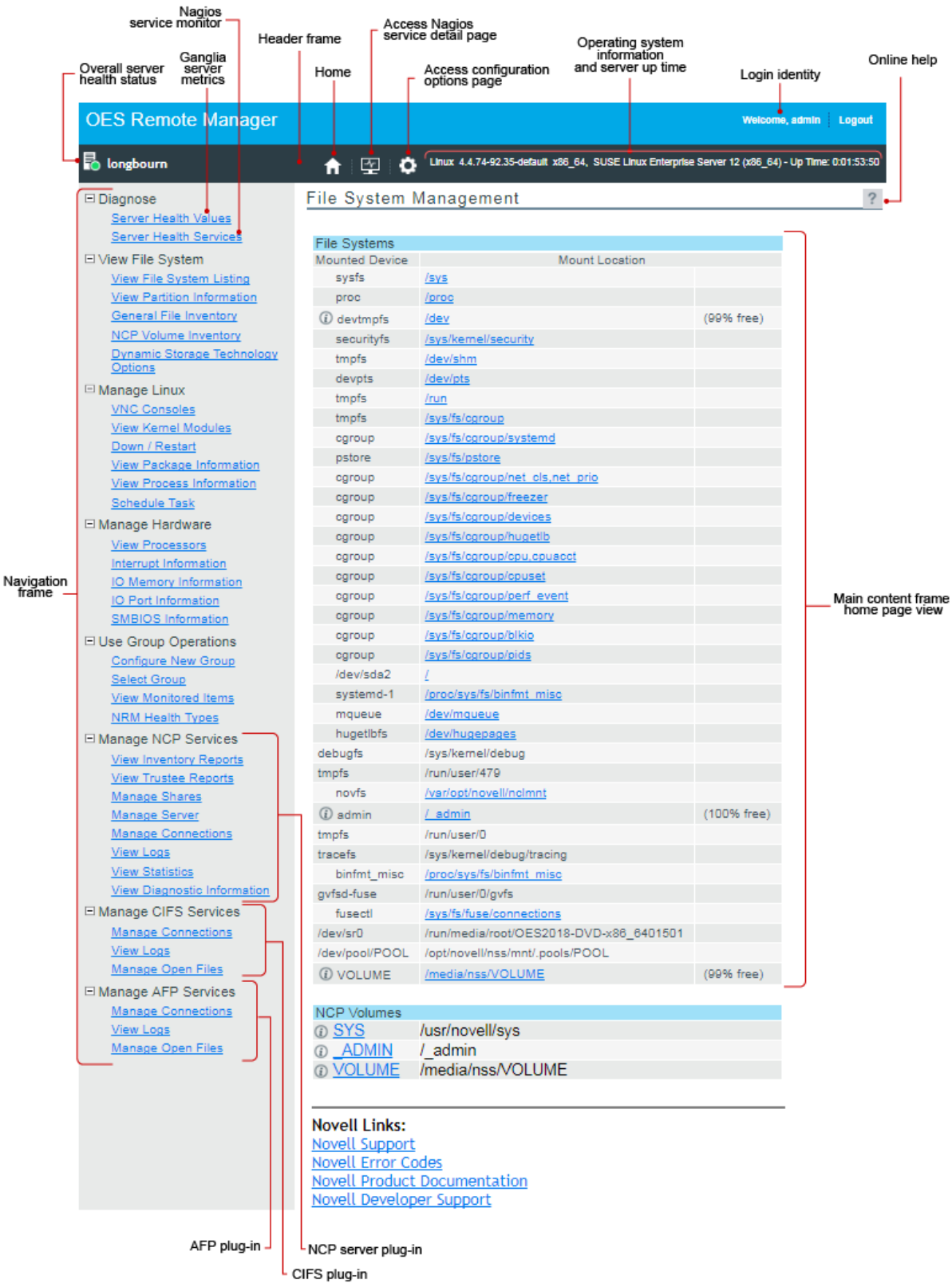
To stop HTTPSTKD	`rcnovell-httpstkd stop`
	or
	`systemctl stop novell-httpstkd.service`

5.4 Understanding the Layout of OES Remote Manager

The web pages for OES Remote Manager have three main frames: the header frame (top), the navigation frame (left), and the main content frame (right). They also contain the **Overall Health Indicator** and online help.

Figure 5-1 on page 25 shows the overall layout of OES Remote Manager.

Figure 5-1 *Layout of OES Remote Manager*



See the following sections for more information about the layout of the OES Remote Manager Home page:

- Section 5.4.1, “Header Frame,” on page 26
- Section 5.4.2, “Overall Health Indicator,” on page 26
- Section 5.4.3, “Navigation Frame,” on page 27
- Section 5.4.4, “Program Plug-Ins in the Navigation Frame,” on page 28
- Section 5.4.5, “Main Content Frame,” on page 28
- Section 5.4.6, “Online Help,” on page 28

5.4.1 Header Frame

The header frame contains the toolbar and general information about the server.

The toolbar buttons link to the following functions:

- **Home**

  The File System Management page is considered the Home page.

- **Health Monitor** (Nagios Service Detail in OES 11 SP2 and later)

  For information about configuring and using Nagios to monitor services, see Section 7.5, “Configuring Nagios,” on page 47.

- **Configuration**

  For information about OES Remote Manager Configuration Options, see Chapter 6, “Changing the HTTPSTKD Configuration,” on page 31.

The general information about the server includes the following:

- Name of the user you logged in as to OES Remote Manager (typically, the `root` user)
- Overall health indicator
- Server hostname
- Version of the Linux kernel running on the server
- Hardware platform
- Operating system running on the server
- Up time for the server (the amount of time the server has been running since the last reboot) in the format of `days:hh:mm:ss`.

5.4.2 Overall Health Indicator

The **Overall Health Indicator** shows the current server health status as good, suspect, bad, or no connection. For OES, the status is determined from the services that you configure to be monitored by Nagios. The indicator changes if any Nagios-monitored service has a problem alert. If there are multiple alerts, the indicator represents the worst reported health condition. You can click the **Server Health** icon (shown in Table 5-2) to go to the Nagios Service Detail page and view the health statistics and alerts for the monitored services. By default, only basic services are set up to be monitored by

Nagios. In order for the **Overall Health Indicator** to consider the health of additional services, you must configure them to be monitored by Nagios. For information about configuring and using Nagios, see Section 7.5, “Configuring Nagios,” on page 47.

Table 5-2 *Overall Server Health Status Conditions*

Overall Health Status	Server Health Icon	Icon Description
Good		Green orb in a white circle
Suspect		Yellow orb in a white circle
Bad		Red orb in a white circle
No connection to the server		Black X in a white circle

5.4.3 Navigation Frame

The navigation frame lists general tasks that you can perform, and provides links to specific pages for performing those tasks. The left navigation frame includes collapsible categories that are remembered the next time you log in. This lets you display the OES Remote Manager features that you use most often and hide some of the ones that you don’t.

IMPORTANT: When you work in OES Remote Manager, you must use the navigation links provided in the tool. Using the browser's **Back** button can result in unintended actions being re-sent to the server.

Basic links in the navigation frame are identified in Table 5-3.

Table 5-3 *Standard Roles in the Navigation Frame*

Roles	Description	For more information, see
Diagnose	Monitor the health of the server and services.	Chapter 7, “Diagnosing Problems Using Ganglia and Nagios,” on page 39
View File System	Browse the file system, view information about files, folders, and partitions, and generate inventories.	Chapter 8, “Viewing File Systems,” on page 65
Manage Linux	View information about kernel modules, packages, and processes. Schedule CRON jobs.	Chapter 9, “Managing Linux,” on page 73
Manage Hardware	View information about processors, interrupts, memory, ports, and SMBIOS.	Chapter 10, “Managing Hardware,” on page 83

Roles	Description	For more information, see
Use Group Operations	Configure groups of servers to be monitored collectively.	Chapter 11, “Using Group Operations,” on page 89

5.4.4 Program Plug-Ins in the Navigation Frame

The links in the navigation frame change depending on the programs installed on the server that have plug-ins to OES Remote Manager. The plug-ins are installed automatically when you install the related OES Services.

Table 5-4 *Program Plug-In Roles in the Navigation Frame*

OES Service	Roles in the Navigation Frame	For more information, see
NCP Server and Dynamic Storage Technology	**Manage NCP Services** allows you to manage NSS volumes, NCP volumes, DST volumes, NCP volume inventories, and NCP connections on the server.	Chapter 12, “Managing NCP Services,” on page 103 *OES 2018 SP3: NCP Server for Linux Administration Guide*
	Dynamic Storage Technology Options allows you to configure and manage Dynamic Storage Technology volumes and policies. The DST functions are integrated with **Manage NCP Services**.	Chapter 13, “Managing Dynamic Storage Technology Options,” on page 131 *OES 2018 SP3: Dynamic Storage Technology Administration Guide*
Novell CIFS	**Manage CIFS Services** allows you to manage OES CIFS connections on the server.	Chapter 14, “Managing CIFS Services,” on page 135 *OES 2018 SP3: OES CIFS for Linux Administration Guide*.
Novell AFP	**Manage AFP Services** allows you to manage OES AFP connections on the server.	Chapter 15, “Managing AFP Services,” on page 139 *OES 2018 SP3: OES AFP for Linux Administration Guide*

5.4.5 Main Content Frame

The information in the main content frame changes depending on which link you click in the header or navigation frame. The File System Management page is considered the Home page.

5.4.6 Online Help

When a **Help** icon ? appears in the upper-right corner of a page in the main content frame, you can view help for the page that is displayed.

5.5 Accessing Configuration Options

Click the Configure icon in the header frame to access the Configuration Options page. Use this page to configure the following:

- HTTP Interface Management
- Nagios Configuration Options (only for OES 11 SP2 and later)
- Restart the Nagios daemon
- Restart the `httpstkd` daemon
- HTTP Logs
- Novell Remote Manager Certificate Management
- Novell Remote Manager Schema Management
- Enable/disable the httpstkd daemon core file

For information about setting options, see Chapter 6, “Changing the HTTPSTKD Configuration,” on page 31.

5.6 Accessing Online Help

Online help, which provides detailed information and instructions for using OES Remote Manager features, is available for most management tasks and settings.

To access the online help, click the **Help** icon ? on the upper right portion of the page or next to the specific item link.

5.7 Accessing Micro Focus Web Pages

Micro Focus links on the Home (File System Management) page provide quick access to the following:

- **Micro Focus Support** (http://www.novell.com/support/) links directly to the Micro Focus Support website, where you can get current server patch kits and updates or find troubleshooting information.
- **Novell Error Codes** (http://www.novell.com/documentation/nwec/index.html) links directly to the information about Novell Error Codes, including what they mean and possible causes and actions for them.
- **Micro Focus Product Documentation** (http://www.novell.com/documentation) links directly to the product documentation for all shipping Micro Focus products.
- **Micro Focus Developer Support** (http://www.novell.com/developer/) links directly to the Novell Developer website, where you can find tips and suggestions beyond the basics for managing, troubleshooting, and diagnosing your server.

6 Changing the HTTPSTKD Configuration

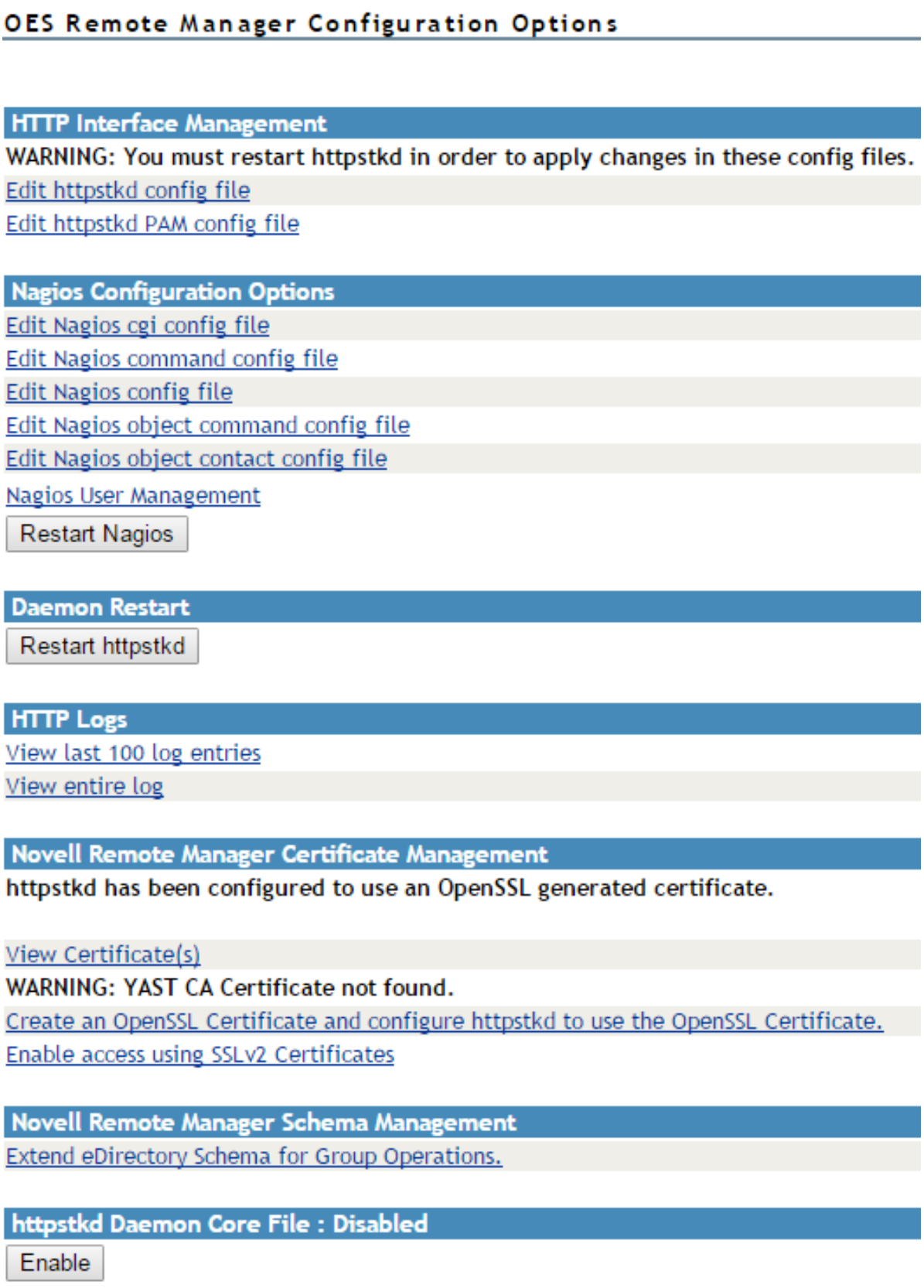
When NRM is installed, it sets up a small web server on your server. The interface and module is called HTTPSTKD. It automatically sets its basic configuration parameters that allow it to work.

You might need to configure NRM after the initial installation for a variety of reasons. For example, you might want to bind additional IP addresses to HTTPSTKD, set up stronger security, or extend the eDirectory schema for Group Monitoring.

You can perform these tasks using the options on the OES Remote Manager Configuration Options page, as shown in Figure 6-1. To access this page, click the **Configure** icon in the header frame.

The Configuration Options page also provides links for **Nagios Configuration Options**. For information about changing the Nagios configuration, see Section 7.5, “Configuring Nagios,” on page 47.

Figure 6-1 *The OES Remote Manager Configuration Options Page*


OES Remote Manager Configuration Options
HTTP Interface Management
WARNING: You must restart httpstkd in order to apply changes in these config files.
Edit httpstkd config file
Edit httpstkd PAM config file
Nagios Configuration Options
Edit Nagios cgi config file
Edit Nagios command config file
Edit Nagios config file
Edit Nagios object command config file
Edit Nagios object contact config file
Nagios User Management
Restart Nagios
Daemon Restart
Restart httpstkd
HTTP Logs
View last 100 log entries
View entire log
Novell Remote Manager Certificate Management
httpstkd has been configured to use an OpenSSL generated certificate.
View Certificate(s)
WARNING: YAST CA Certificate not found.
Create an OpenSSL Certificate and configure httpstkd to use the OpenSSL Certificate.
Enable access using SSLv2 Certificates
Novell Remote Manager Schema Management
Extend eDirectory Schema for Group Operations.
httpstkd Daemon Core File : Disabled
Enable

On this page you can perform the following tasks:

- Section 6.1, “Accessing and Editing the HTTPSTKD Configuration File,” on page 33
- Section 6.2, “Accessing and Editing the HTTPSTKD PAM Configuration File,” on page 34
- Section 6.3, “Restarting the HTTPSTKD Daemon,” on page 35
- Section 6.4, “Viewing the HTTP Logs,” on page 35
- Section 6.5, “Viewing and Creating Certificates for OES Remote Manager,” on page 36
- Section 6.6, “Extending the eDirectory Schema for OES Remote Manager Group Operations,” on page 37

6.1 Accessing and Editing the HTTPSTKD Configuration File

Anytime you want to change the functionality of OES Remote Manager, access the `/etc/opt/novell/httpstkd.conf` file, modify the settings, then restart the HTTPSTKD daemon.

NOTE: Beginning with OES 2018 SP3, NRM supports communication over TLS v1.2 when the cipher level in the /etc/opt/novell/httpstkd.conf file is set to all or high.

To access and edit this file from within OES Remote Manager:

1. Log in to OES Remote Manager as the `root` user.
2. Click the **Configure** icon in the navigation frame.
3. Click **Edit httpstkd config file**.
4. Make the changes.
5. Click **Save Changes**.

You can alternatively open the `/etc/opt/novell/httpstkd.conf` file in a text editor that saves files to a UNIX format, edit the file, then save the file.

After making changes to this file and saving it, restart the HTTPSTKD daemon. See “Restarting the HTTPSTKD Daemon” on page 35. You can also restart it manually as described in Section 5.3, “Starting or Stopping HTTPSTKD,” on page 23.

Table 6-1 identifies the functions that are controlled by settings in the OES Remote Manager configuration file, and provides links to information about how to change them.

Table 6-1 *Information for Changing the Functionality of OES Remote Manager*

Functionality	Information about How to Change
Which network adapter OES Remote Manager is bound to or add additional IP address that it is bound to	Section A.1, “Address and Port Commands,” on page 157
The certificates OES Remote Manager is using for authentication	◆ Section 6.5, “Viewing and Creating Certificates for OES Remote Manager,” on page 36 ◆ Section A.1, “Address and Port Commands,” on page 157

Functionality	Information about How to Change
The cipher strength of the SSL key that is used to access OES Remote Manager	Section A.8, “SSL Key Cipher Strength Command,” on page 165
The HttpOnly attribute for cookies in a response header	Section A.4, “HttpOnly Command,” on page 161
The `InventoryResolveNonLumOwnerName` option for resolving names of NSS volume file owners if their eDirectory user names are not LUM enabled	Section A.5, “InventoryResolveNonLumOwnerName Command,” on page 162
Which plug-ins are loaded	Section A.7, “Load Command,” on page 164
Which workstations can access OES Remote Manager	Section A.3, “Filtering Commands,” on page 160
Which users can log in to OES Remote Manager	◆ Section A.2, “Disable Auto LUM Command,” on page 158 ◆ Section A.9, “Supervisor Only Command,” on page 165
The language the browser supports	Section A.6, “Language Commands,” on page 162

6.2 Accessing and Editing the HTTPSTKD PAM Configuration File

Linux uses PAM (Pluggable Authentication Modules) in the authentication process as a layer that mediates between user and application. PAM modules are available on a system-wide basis, so they can be requested by any application.

Every program that relies on the PAM mechanism has its own configuration file in the directory `/etc/pam.d/`*`program_name`*. These files define the PAM modules that are used for authentication. In addition, there are global configuration files for most PAM modules under `/etc/security` directory, which define the exact behavior of these modules (examples are `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, and `time.conf`). Every application that uses a PAM module actually calls a set of PAM functions, which then processes the information in the various configuration files and returns the results to the calling application.

This file controls the authentication to NRM on an OES Linux server. The default configuration should work. If you want to change the way your users authenticate to NRM, you can edit this file.

These are the lines that enable NRM integration with user management:

```
auth       sufficient pam_nam.so
account    sufficient pam_nam.so
password   sufficient pam_nam.so
session    optional   pam_nam.so
```

To access and edit this file from within OES Remote Manager:

1. Log in to OES Remote Manager as the `root` user.
2. In OES Remote Manager, click the **Configure** icon in the navigation frame.
3. Click **Edit httpstkd PAM config file**.

4 Make the changes.

5 Click **Save Changes**.

6 After making changes to this file, restart the HTTPSTKD daemon. See "Restarting the HTTPSTKD Daemon" on page 35.

You can alternatively use an editor that saves files to a UNIX format to edit the `/etc/pam.d/httpstkd` file. After changing the file, restart the HTTPSTKD daemon. See "Restarting the HTTPSTKD Daemon" on page 35.

For more information about the PAM configuration file and the options available, see "Authentication with PAM" (https://www.suse.com/documentation/sles-12/book_security/data/cha_pam.html) in the *SUSE Linux Enterprise Server 12 Security Guide* (https://www.suse.com/documentation/sles-12/book_security/data/book_security.html).

6.3 Restarting the HTTPSTKD Daemon

After making changes to the HTTPSTKD configuration file or the HTTPSTKD PAM configuration file, restart the HTTPSTKD daemon.

To restart the HTTPSTKD daemon, click **Restart httpstkd** on the OES Remote Manager Configuration Options page.

You can also restart it manually. See "Starting or Stopping HTTPSTKD" on page 23.

6.4 Viewing the HTTP Logs

The OES Remote Manager Configuration Options page contains a link for all the HTTPSTK-related messages contained in the `/var/log/messages` file.

This information is valuable for seeing who logged in through OES Remote Manager, when they logged in, the pages being viewed, log failures, and so on.

You can view the last 100 entries of the log or the entire log.

To view this log:

1 Click the **Configure** icon in the navigation frame.

2 Under the **HTTP Logs** heading, click either **View last 100 log entries** or **View entire log**.

The logging to this file is controlled by the Syslog options. To change these default syslog options, edit the `etc/sysconfig/syslog` file.

6.5 Viewing and Creating Certificates for OES Remote Manager

OES Remote Manager uses the default certificates created during the installation to secure access through it to the server. This certificate is bound to the first network board found in the server configuration.

During the install of eDirectory on a new server installation, there is a check box to have all HTTP services use an eDirectory certificate. HTTPSTKD uses that certificate if this check box is selected or the YAST CA certificate if it is not selected. On upgrades, the check box in eDirectory is not selected, so certificates that were previously used are maintained.

You can create new certificates and modify the `/etc/opt/novell/httpstkd.conf` file to use any certificates other than the default certificate file for any reason. You should create a new certificate in cases such as the following:

- The default certificate does not meet the level of security required by your organization
- The default certificate was bound to a DHCP address
- You have changed the server's IP address
- You want to bind a new certificate to a different network board

To view the certificates being used:

1. Click the **Configure** icon in the navigation frame.
2. Under the **Novell Remote Manager Certificate Management** heading, click **View Certificate(s)**.

To create a new certificate:

1. Click the **Configure** icon in the navigation frame.
2. Under the **Novell Remote Manager Certificate Management** heading, click **Create Certificate**.
3. On the Create a Certificate for OES Remote Manager page, specify the required information in the **Certificate Information** fields.

   This creates a new certificate and automatically replaces the current certificate at `/etc/opt/novell/httpstkd/server.pem`.

   If you want to create the certificate in a different location or with a different name, change the file name or path in the **Certificate File** field.
4. Click **Create**.
5. (Conditional) If you changed the name of the certificate file or the path to it from the default location, edit the `/etc/opt/novell/httpstkd.conf` before restarting HTTPSTKD.
6. Restart HTTPSTKD by clicking the **Restart Httpstkd** button on the OES Remote Manager Configuration Options page.

To bind NRM to an additional IP address to or to a different certificate:

1. Click the **Configure** icon in the navigation frame.
2. Click **Edit Httpstkd Config File**.

3 In the Address and Port portion of the file, specify the new IP address or certificate path and name.

For example, if you had two network boards that you wanted to bind NRM to, you would create or have two separate certificates and then make these entries in the `/etc/opt/novell/httpstkd.conf` file:

```
addr 192.27.1.123:8008
addr 192.27.1.123:8009 keyfile=/etc/opt/novell/httpstkd/server.key
certfile=/etc/opt/novell/httpstkd/server1.pem

addr 192.27.1.124:8008
addr 192.27.1.124:8009 keyfile=/etc/opt/novell/httpstkd/server.key
certfile=/etc/opt/novell/httpstkd/server2.pem
```

You can put the certificate in any location as long as the entry in the `/etc/opt/novell/httpstkd.conf` points to the correct location and file name.

6.6 Extending the eDirectory Schema for OES Remote Manager Group Operations

When you use Group Operations and want to save the groups that you have created, OES Remote Manager requires you to save the file on the server locally or assign it to an eDirectory object.

Before you can save it to an eDirectory object, you must extend the eDirectory schema to access the attributes for OES Remote Manager group operations at least once in the eDirectory tree that you are saving to.

You can do this easily by clicking either the **Extend eDirectory Schema for Group Operations** link on the **OES Remote Manager Configuration Options** page any time before you create a group or the link in the failure error message displayed when saving the group. As with all schema extensions, you must have the necessary rights to extend the schema.

The message `NDS schema extension complete` is displayed on this page when the operation is done. Then you can save the group.

7 Diagnosing Problems Using Ganglia and Nagios

OES Remote Manager includes several tools to assist you in monitoring the health and status of your server and services. Beginning with Open Enterprise Server (OES) 11 SP2, OES Remote Manager uses the open source monitoring tools Ganglia and Nagios to monitor the health of the server and the services and applications running on it. The tools provide complementary health monitoring functions. Ganglia gathers server metrics and tracks trends over time. Nagios monitors health and provides an alert and notification system. You can use these tools to become familiar with the normal health and status of your server. They can help you identify and diagnose problems with your server.

IMPORTANT: The Health Monitor function in OES Remote Manager is obsoleted in OES 11 SP2 and later. It is replaced by the Ganglia and Nagios open source monitoring tools, which do not use the Small Footprint CIM Broker (SFCB) for communications.

Performing the following tasks can help you to become familiar with the health and status of your servers:

- Section 7.1, “Monitoring Server Health,” on page 40
- Section 7.2, “Configuring Ganglia,” on page 40
- Section 7.3, “Stopping and Starting Ganglia gmond and gmetad,” on page 44
- Section 7.4, “Monitoring Server Health with Ganglia,” on page 44
- Section 7.5, “Configuring Nagios,” on page 47
- Section 7.6, “Monitoring Service Health with Nagios,” on page 55
- Section 7.7, “Restarting Nagios,” on page 55
- Section 7.8, “Managing Nagios Users,” on page 56
- Section 7.9, “Modifying the Nagios Notification Methods for Contacts,” on page 58
- Section 7.10, “Configuring Nagios Logging,” on page 59
- Section 7.11, “Viewing the PIDs or Monitoring the Health of Processes,” on page 61
- Section 7.12, “Monitoring or Killing an Individual Process,” on page 62
- Section 7.13, “Troubleshooting a Suspect or Bad Health Status,” on page 63

7.1 Monitoring Server Health

Monitoring the health of your server can help prevent it from getting to a state in which your users cannot access the server or the data on it. OES Remote Manager allows you to monitor the server's overall health and the health of a specific item.

- Section 7.1.1, "Viewing the Overall Server Health Status," on page 40

7.1.1 Viewing the Overall Server Health Status

The server's overall health is indicated by the color of the circle displayed next to the **Server** icon in the header frame for OES Remote Manager. The following table lists and explains each health status that might be displayed.

Table 7-1 *Server Health Status*

Icon	Server Health Status	Explanation
	Good	All parameters included in the server's health configuration list are good.
	Suspect	The status of one or more of the parameters included in the server's health configuration list is suspect or has a minor problem.
	Bad	The status of one or more of the parameters included in the server's health configuration list is bad or has a critical problem.
	Lost connection	The connection to the server from OES Remote Manager has been lost.

The server's overall health is determined by services that you configure to be monitored by Nagios.

If the status of any Nagios-monitored service changes to yellow (suspect) or red (bad), the health status indicator light in the header frame changes to indicate there is a problem. If more than one item changes, the worst status indicates the server's overall status. When the status for all items returns to green (good), then the health light indicator changes back to green (good).

7.2 Configuring Ganglia

Ganglia is an open source monitoring tool that collects server metrics and graphically displays their trends over the past hour, day, week, month, or year. It shows similar graphs for memory usage, disk usage, network statistics, number of running processes, and all other Ganglia metrics. The Ganglia Monitoring daemon (`gmond`) has a low overhead and does not impact user performance.

The Ganglia UI has embedded help to guide you in using the services on each tab. For additional information, see *Ganglia Monitoring System* (http://ganglia.info) on the web.

- Section 7.2.1, "Ganglia Requirements," on page 41
- Section 7.2.2, "Configuring Ganglia gmond in Multicast Mode or Unicast Mode," on page 42

7.2.1 Ganglia Requirements

Ganglia requires the following settings in order to display the server health statistics:

- "Port 8649" on page 41
- "Time Synchronization" on page 41

Port 8649

If a firewall is enabled on the server, you must open port 8649 in order to use Ganglia. By default, the gmond daemon communicates on UDP port 8649, and the gmetad daemon downloads metrics data over TCP port 8649. The port is specified in udp_send_channel, udp_recv_channel, and tcp_accept_channel parameters in the /etc/opt/novell/ganglia/monitor/gmond.conf file. If you have firewall rules that block traffic on those ports, your metrics do not show up in the monitoring dashboard. You must restart the Ganglia gmond and gmetad daemons after you open the port in the firewall.

1. Log in to the server as the Linux root user, then open a terminal console.
2. Open port 8649 in the firewall. Enter

   ```
   SuSEfirewall2 open EXT UDP 8649
   SuSEfirewall2 open EXT TCP 8649
   ```

3. Restart gmond and gmetad. Enter

   ```
   systemctl stop novell-gmond.service
   systemctl stop novell-gmetad.service
   systemctl start novell-gmetad.service
   systemctl start novell-gmond.service
   ```

Time Synchronization

If your Ganglia server monitors the health of multiple computers, ensure that the time on the gmond server is correct and matches the gmetad that is collecting data. The timestamp used to update the gmetad round-robing database (RRD) files are in the Universal Time Coordinated (UTC) standard, which is the international time standard.

Consider using the same Network Time Protocol (NTP) time source on the group of machines in order to keep their time synchronized. NTP is an industry standard. It ensures accurate timekeeping by synchronizing clocks to UTC time. If a firewall is enabled on the servers, ensure that you open the firewall on UDP port 123 to allow NTP traffic. After you configure NTP, delete the current gmetad round-robin databases (RRDs) in the /var/opt/novell/ganglia/rrds subdirectories, and then restart gmond and gmetad.

1. Log in to the server as the Linux root user, then open a terminal console.
2. Open port 123 in the firewall. Enter

   ```
   SuSEfirewall2 open EXT UDP 123
   ```

3. Configure NTP on the server.

   For information about configuring NTP, see "Time Services" in the *OES 2018 SP3: Planning and Implementation Guide*.

4 In a file browser, delete the current gmetad round-robin databases (RRDs) in the /var/opt/novell/ganglia/rrds directory.

5 Restart gmond and gmetad. Enter

```
systemctl stop novell-gmond.service
systemctl stop novell-gmetad.service
systemctl start novell-gmetad.service
systemctl start novell-gmond.service
```

7.2.2 Configuring Ganglia gmond in Multicast Mode or Unicast Mode

Ganglia uses the gmond daemon to gather health monitoring statistics. It keeps a cache of all metrics in memory. Ganglia uses the gmetad daemon to periodically poll the gmond daemon to store the metrics in a storage engine. By default, OES Remote Manager configures Ganglia in multicast mode. Both the gmond daemon and the gmetad run on the same server.

The gmond daemon can alternatively be configured in unicast mode. You can also configure it to monitor in groups of servers, called Ganglia clusters. For more information, see the *Ganglia Quick Start Guide* (http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_quick_start) on the Ganglia Project (http://sourceforge.net/apps/trac/ganglia/) website.

- "Using Ganglia in Multicast Mode" on page 42
- "Using Ganglia in Unicast Mode" on page 43
- "Configuring gmond for Server-Centric Monitoring" on page 43

Using Ganglia in Multicast Mode

By default, the Ganglia gmond daemon is configured in multicast mode, and that is how it is installed for OES Remote Manager. Ganglia settings for gmond are in the /etc/opt/novell/ganglia/monitor/gmond.conf file.

The gmond daemon's global parameters are set for it to be both a sender (mute=no) and a receiver (deaf=no). The gmond daemon aggregates all metrics sent to it from other hosts running Ganglia in the same IP subnet, or in the same Ganglia cluster (if configured). There is no need to list every single host, because a gmond set in receive mode automatically contains the list of all hosts and metrics in the subnet (or in the same Ganglia cluster, if configured). Metrics and their metadata (metric groups, types and so on) are sent separately. If Ganglia is restarted while using multicast mode, gmond servers can talk to each other, and will ask for metadata if it is missing.

Ganglia settings for gmetad are in the /etc/opt/novell/ganglia/monitor/gmetad.conf file. Its root directory for the round-robin databases (RRDs) is the /var/opt/novell/ganglia/rrds directory. The data source for the localhost is named Grid-Node, and its metrics RRD files are found in the /var/opt/novell/ganglia/rrds/Grid-Node directory.

You can turn off multicasting to view statistics only for the single server where you are logged in to OES Remote Manager. For more information, see "Configuring gmond for Server-Centric Monitoring" on page 43.

Using Ganglia in Unicast Mode

Unicast mode has less traffic than multicast mode does, but it is more complex to configure. In unicast mode, the default behavior for handling metadata is as follows:

- The gmond daemon sends metadata only when it is started.
- If Ganglia is restarted while using unicast mode, metadata is discarded and its corresponding metrics data are also discarded.
- Ganglia does not ask for metadata if it is missing.

The unicast behavior might result in blank graphs on the host-view page if the collecting gmond is restarted while working in unicast mode. Restarting all of the non-collector gmond daemons makes the metric graphs reappear; however, this might not be feasible for large Ganglia clusters. If you use the unicast mode to monitor multiple servers, you should enable the global parameter `send_metadata_interval` in the `/etc/opt/novell/ganglia/monitor/gmond.conf` file, and set it to something other than 0. A setting of 30 to 60 seconds works in most environments. Setting this variable to a non-zero value makes the gmond processes periodically announce their metrics, and the graphs reappear on the host-view page.

For more information about configuring Ganglia in unicast mode, see the *Ganglia Quick Start Guide* (http://sourceforge.net/apps/trac/ganglia/wiki/ganglia_quick_start) on the Ganglia Project (http://sourceforge.net/apps/trac/ganglia/) website.

Configuring gmond for Server-Centric Monitoring

You can modify the `/etc/opt/novell/ganglia/monitor/gmond.conf` file to set up Ganglia to monitor only its own statistics as a single server.

1. Log in to the server as the `root` user.
2. Open the `/etc/opt/novell/ganglia/monitor/gmond.conf` file in a text editor.
3. Find the section `udp_send_channel` and replace it with the following:

   ```
   udp_send_channel {
     #bind_hostname = yes
     #mcast_join = 239.2.19.61
     port = 8649
     #ttl = 1
   }
   ```

   You comment out the `mcast_join` parameter and the `ttl` parameter.
4. Find the section `udp_recv_channel` and replace it with the following:

   ```
   udp_recv_channel {
     #mcast_join = 239.2.19.61
     port = 8649
     #bind = 239.2.19.61
   }
   ```

   You comment out the `mcast_join` parameter and the `bind` parameter.
5. Save and close the file.

6 Open a terminal console, and then stop and start both gmond and gmetad:

```
systemctl stop novell-gmond.service
systemctl stop novell-gmetad.service

systemctl start novell-gmetad.service
systemctl start novell-gmond.service
```

7.3 Stopping and Starting Ganglia gmond and gmetad

1 Log in to the server as the Linux root user, then open a terminal console.

2 Restart gmond and gmetad. Enter

```
systemctl stop novell-gmond.service
systemctl stop novell-gmetad.service

systemctl start novell-gmetad.service
systemctl start novell-gmond.service
```

7.4 Monitoring Server Health with Ganglia

The **Diagnose > Server Health Values** task presents the Ganglia Web interface in the OES Remote Manager browser frame. You can use this page to monitor your server's health statistics. The Ganglia UI has embedded help to guide you in using the services on each tab. For additional information, see *Ganglia Monitoring System* (http://ganglia.info) on the web.

1 Access the Ganglia dashboard, using one of the following methods:

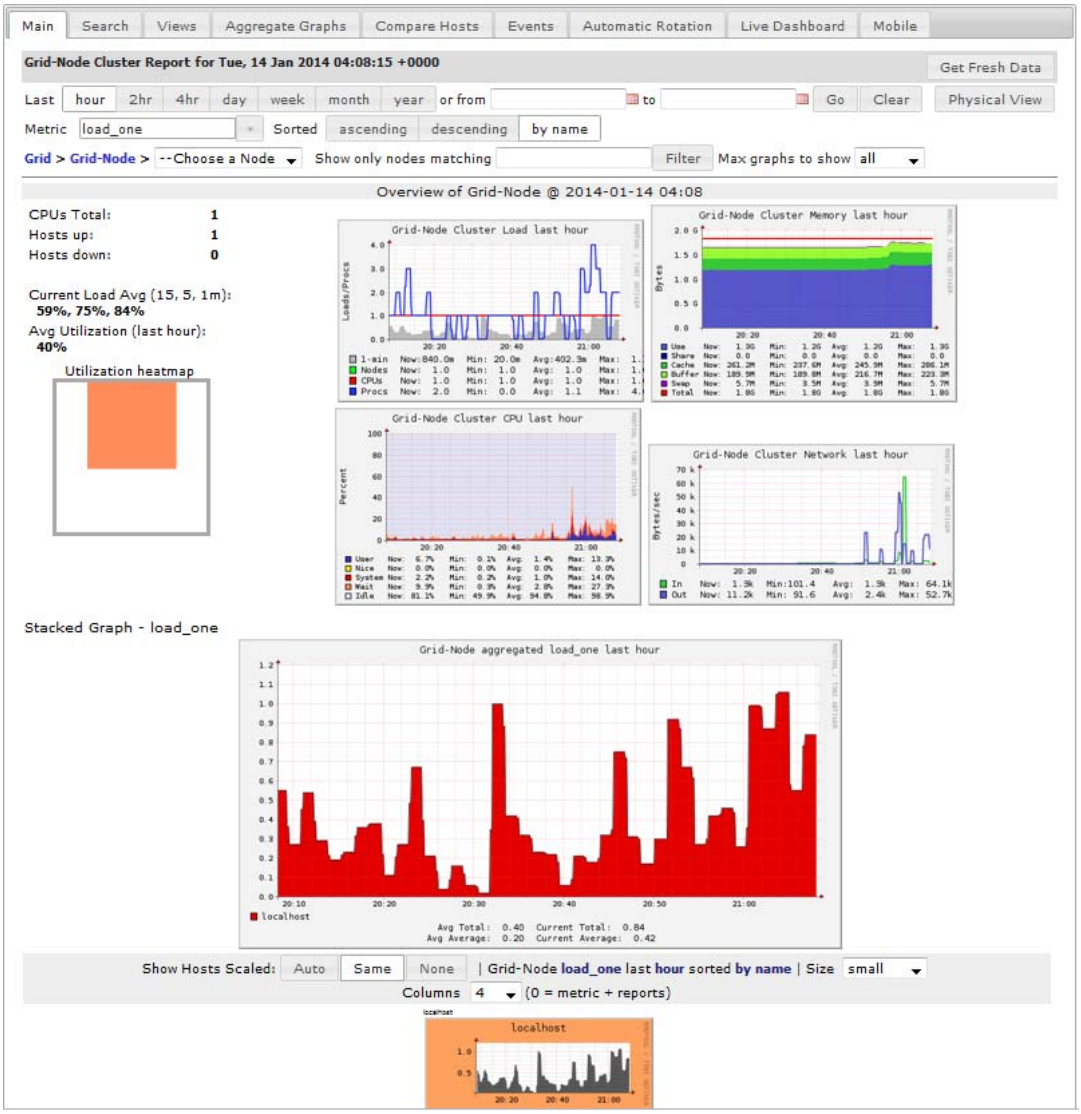
- Log in to OES Remote Manager as the Linux root user or as a LUM-enabled administrator user.
- Select **Diagnose > Server Health Values** to go to the Ganglia main dashboard. Continue to Step 2 on page 45.

or

- In a web browser, go to the Ganglia URL:

  `http://<server_ip_address>/gweb`

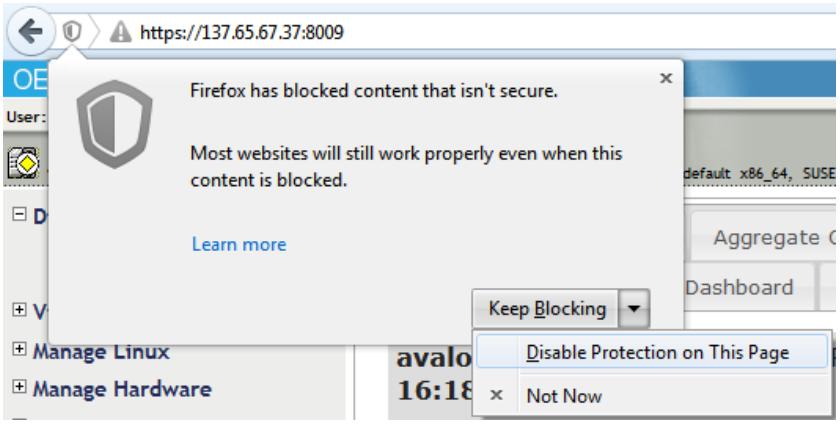
Continue to Step 3 on page 47.


Main
Search
Views
Aggregate Graphs
Compare Hosts
Events
Automatic Rotation
Live Dashboard
Mobile
Grid-Node Cluster Report for Tue, 14 Jan 2014 04:08:15 +0000
Get Fresh Data
Last hour 2hr 4hr day week month year or from to Go Clear Physical View
Metric load_one Sorted ascending descending by name
Grid > Grid-Node > --Choose a Node Show only nodes matching Filter Max graphs to show all
Overview of Grid-Node @ 2014-01-14 04:08
CPUs Total: 1
Hosts up: 1
Hosts down: 0
Current Load Avg (15, 5, 1m):
59%, 75%, 84%
Avg Utilization (last hour):
40%
Utilization heatmap
Grid-Node Cluster Load last hour
Grid-Node Cluster Memory last hour
Grid-Node Cluster CPU last hour
Grid-Node Cluster Network last hour
Stacked Graph - load_one
Grid-Node aggregated load_one last hour
localhost
Show Hosts Scaled: Auto Same None | Grid-Node load_one last hour sorted by name | Size small
Columns 4 (0 = metric + reports)
localhost

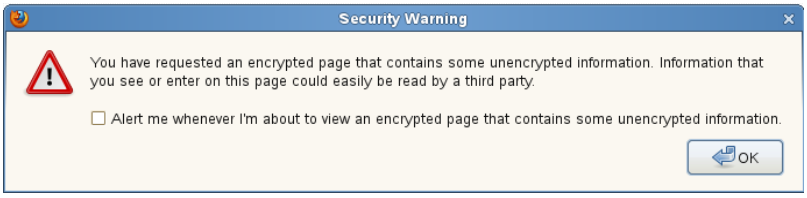
2 If you are prompted with a security warning that the page contains mixed content (both secure and non-secure elements), select the option to show all content.

The OES Remote Manager frame sends secure content. However, Ganglia uses scripts to graphically display statistics that send the statistical data via HTTP instead of HTTPS. Depending on how your web browser is configured to handle mixed content on a web page, the Ganglia statistics might not be displayed in the graph windows.

- **Firefox:** In Firefox 23 and later, when you access a page with both HTTPS and HTTP content, a shield icon appears in the address bar, and the browser automatically blocks certain content such as non-secure scripts. To allow mixed content, right-click the shield icon, then select **Disable Protection on This Page**. After you disable protection, an orange alert icon appears in the address bar and makes you aware that the displayed page contains mixed content.



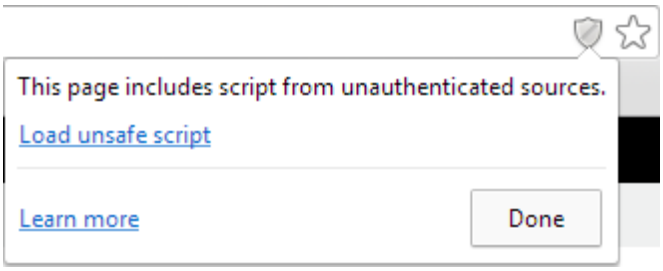
In a Mozilla Firefox 22 and earlier web browser, you receive a warning, but content is not automatically blocked. A **Security Warning** pop-up dialog box reports: `You have requested an encrypted page that contains some unencrypted information`. Click **OK** to dismiss the warning and allow mixed content to be displayed.


Security Warning
You have requested an encrypted page that contains some unencrypted information. Information that you see or enter on this page could easily be read by a third party.
Alert me whenever I'm about to view an encrypted page that contains some unencrypted information.
OK

A round shield icon replaces the lock to the left of the https:// in the address bar. Right-click the icon to view the message that advises: `Your connection to this site is only partially encrypted, and does not prevent eavesdropping`.

- **Internet Explorer:** In a Microsoft Internet Explorer web browser, the pop-up dialog box is displayed at the bottom of the page and reports: `Only secure content is displayed`. Click **Show all content** to dismiss the warning and allow mixed content to be displayed.

- **Chrome:** In a Google Chrome web browser, a shield appears at the end of the URL in the address bar. It warns: `This page includes scripts from unauthenticated resources`. Right-click the shield, then click **Load Unsafe Script**.



While mixed content is displayed in Chrome, the green text `https://` and lock in the URL https://, which indicates secure-only content, is automatically changed to red text that is crossed out and a gray lock with a red X https://.

3 Select any of the following tabs to search, configure events to monitor, or define reports:

- Search
- Views
- Aggregate Graphs
- Compare Hosts
- Events
- Automatic Rotation
- Live Dashboard
- Mobile

7.5 Configuring Nagios

Nagios is an open source monitoring tool. You can configure it to monitor the health of the server systems and services. It also provides an alert and notification system.

The information in this section provides basic information to get you started using Nagios. For detailed information about configuring and using Nagios to monitor your server and services, see other sections in this guide. See also the open source *Nagios Documentation* (http://www.nagios.org/documentation) at Nagios.org.

- Section 7.5.1, “Configuring Nagios Authenticated Users and Contacts,” on page 47
- Section 7.5.2, “Configuring Nagios Monitoring,” on page 51
- Section 7.5.3, “Accessing the Nagios Website,” on page 53
- Section 7.5.4, “Using Nagios Plug-Ins,” on page 54
- Section 7.5.5, “Using Object Configuration Files,” on page 54
- Section 7.5.6, “Additional Information,” on page 54

7.5.1 Configuring Nagios Authenticated Users and Contacts

Nagios user accounts are specific to the Nagios software. The accounts have nothing to do with the local server user names or eDirectory user names.

There are two levels of access for Nagios users:

- **Authenticated user:** a Nagios user who is granted access to the web-based Nagios monitoring dashboard.
- **Authenticated contact:** An authenticated Nagios user whose user name is also defined in the Nagios Object Contact configuration file (`/etc/nagios/objects/contacts.cfg`) and has permissions to access CGI information as defined in the Nagios CGI configuration file (`/etc/nagios/cgi.cfg`) and other object configuration for services that are monitored.

By default, the Nagios user `nagiosadmin` is already configured in Nagios as a user, a contact, and a member of the contact group `admins`. This user is also authorized to access server and services information and to issue host or service commands via the command CGI configuration file (`/etc/`

nagios/cgi.cfg). However, you must configure a password for the nagiosadmin user in order to log in to the **Nagios Service Details** website. You must configure a valid email address for the nagiosadmin contact in order to receive alerts via the Nagios alert notification system.

- "Setting or Modifying the Password for the nagiosadmin User" on page 48
- "Setting or Modifying an Email Address for the nagiosadmin Contact" on page 49
- "Using the Nagios admins Contact Group" on page 51

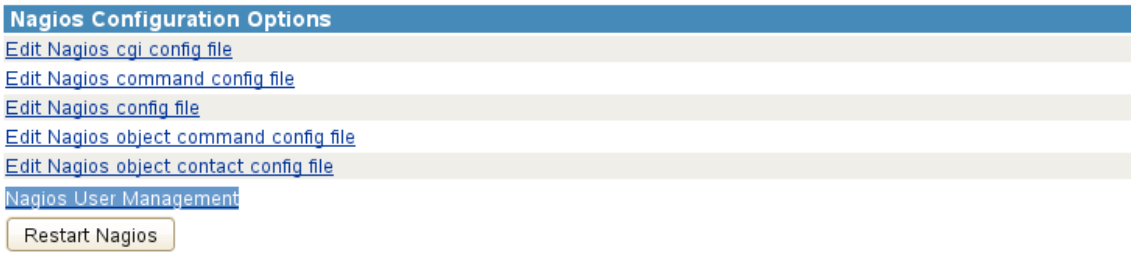
Setting or Modifying the Password for the nagiosadmin User

By default, Nagios defines one default user nagiosadmin with no password in the /etc/nagios/htpasswd.users file. OES Remote Manager requires passwords to be set for any Nagios user. Thus, before you can access the web-based Nagios Service Details report for the first time, you must specify a password to use for the user nagiosadmin.

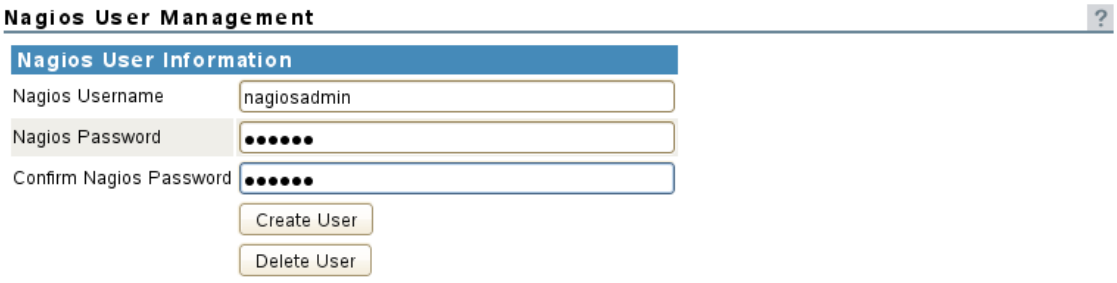
IMPORTANT: Do not delete the nagiosadmin user.

To configure a password for user nagiosadmin:

1. Log in to OES Remote Manager as the Linux root user.
2. Click the **Configure** icon in the toolbar to go the OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Nagios User Management**.


Nagios Configuration Options
Edit Nagios cgi config file
Edit Nagios command config file
Edit Nagios config file
Edit Nagios object command config file
Edit Nagios object contact config file
Nagios User Management
Restart Nagios

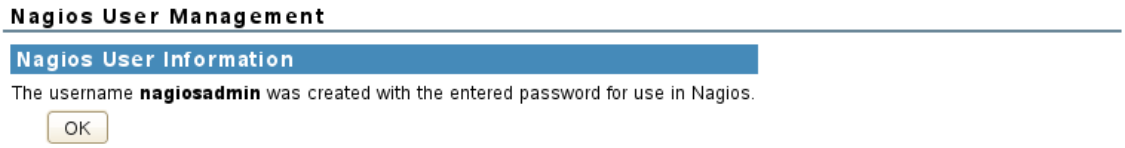
4. On the Nagios User Management page, specify nagiosadmin as the Nagios user name.



5. Type a password, then type it again to confirm.
6. Click **Create User**.

   The user name and password are saved in the /etc/nagios/htpasswd.users file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.

7 When a message confirms that the user nagiosadmin was created in Nagios with the password you provided, click **OK** to dismiss the message.


Nagios User Management
Nagios User Information
The username nagiosadmin was created with the entered password for use in Nagios.
OK

For information about configuring additional Nagios users and the tasks they can perform, see Section 7.8, “Managing Nagios Users,” on page 56.

Setting or Modifying an Email Address for the nagiosadmin Contact

By default, Nagios defines the nagiosadmin user as a contact in the /etc/nagios/objects/contacts.cfg file. It sets the email for the contact to nagios@localhost. In order to receive notification alerts from the Nagios alert notification system, you must replace this email setting with a valid email address. You must restart Nagios to apply the changes.

IMPORTANT: Do not delete the nagiosadmin contact or its email definition line in the /etc/nagios/objects/contacts.cfg file.

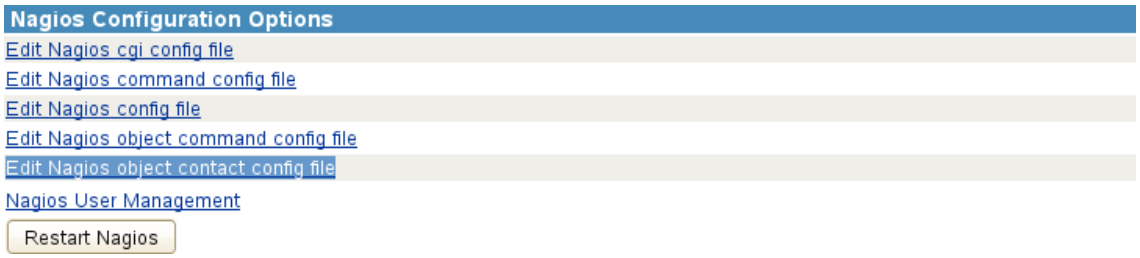
To configure an email address for the contact nagiosadmin:

1 Log in to OES Remote Manager as the Linux root user.

2 Click the **Configure** icon in the toolbar to go the OES Remote Manager Configuration Options page.

3 Under **Nagios Configuration Options**, click **Edit Nagios object contact config file**.

This opens the /etc/nagios/objects/contacts.cfg file in the OES Remote Manager text editor.


Nagios Configuration Options
Edit Nagios cgi config file
Edit Nagios command config file
Edit Nagios config file
Edit Nagios object command config file
Edit Nagios object contact config file
Nagios User Management
Restart Nagios

4 Scroll down to the contact definition section for nagiosadmin, and then replace nagios@localhost with the email address (such as bob@example.com) where you want to receive alert notifications that are sent to nagiosadmin.

/etc/nagios/objects/contacts.cfg

```
##############################################################################
##############################################################################
#
# CONTACTS
#
##############################################################################
##############################################################################

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-
contact'
# template which is defined elsewhere.

define contact{
        contact_name                    nagiosadmin             ; Short name of user
        use                             generic-contact         ; Inherit default
values from generic-contact template (defined above)
        alias                           Nagios Admin            ; Full name of user

        email                           bob@example.com ; <<***** CHANGE THIS TO
YOUR EMAIL ADDRESS ******
        }



##############################################################################
```

Save Changes File Encoding: ANSI UTF-8

5 Click **Save Changes**.

The changes are saved in the `/etc/nagios/objects/contacts.cfg` file. You can verify the new saved date for the file.

/etc/nagios/objects

Upload Text Search Inventory

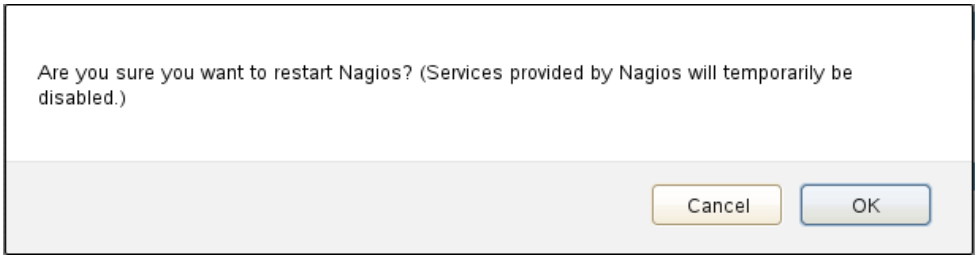
Directory Listing

Info	Name	Size	Date and time	Attributes
	.	N/A	Wed 29 Mar 2017 06:45:11 PM IST	d rwx r.x r.x
	..	N/A	Wed 29 Mar 2017 06:45:11 PM IST	d rwx r.x r.x
	commands.cfg	7,712	Mon 27 Mar 2017 09:32:22 PM IST	. rw. r.. r..
	contacts.cfg	2,166	Mon 27 Mar 2017 09:32:22 PM IST	. rw. r.. r..
	localhost.cfg	5,403	Mon 27 Mar 2017 09:32:22 PM IST	. rw. r.. r..

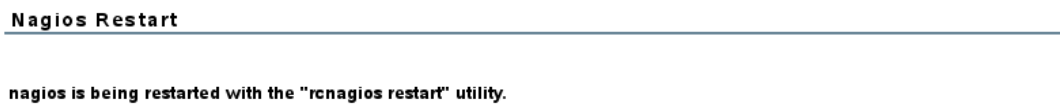
6 Click the **Configure** icon in the toolbar to return to the OES Remote Manager Configuration Options page, then restart Nagios.

6a Under **Nagios Configuration Options**, click **Restart Nagios**.

6b When you are prompted to confirm the restart, click **OK** to proceed.



6c Wait while Nagios is restarted with the `rcnagios restart` utility.



When the restart is completed, OES Remote Manager returns to the Configuration Options page.

Using the Nagios admins Contact Group

Nagios defines a default contact group `admins` and adds the contact `nagiosadmin` as a member of the group in the `contactgroup` section of the `/etc/nagios/objects/contacts.cfg` file.

If you create additional Nagios users and contacts, you can add them to the `admins` group. It is not necessary to create additional contact groups. However, Nagios also allows you to create other contact groups to make it easier to set up authorizations for Nagios users who have different roles.

IMPORTANT: Do not remove the default contact group `admins` from the `/etc/nagios/objects/contacts.cfg` file. Do not remove the Nagios contact `nagiosadmin` from the group `admins`.

You can set up contacts, contact groups, and members of contact groups in the **Nagios Object Contact** configuration file on the OES Remote Manager Configuration Options page (or in the `/etc/nagios/objects/contacts.cfg` file). You must restart Nagios to apply the changes.

7.5.2 Configuring Nagios Monitoring

Nagios is automatically configured with basic monitoring settings for the server. The Nagios contact `nagiosadmin` has all the necessary authorizations to manage and use Nagios.

You can also define other Nagios users and set them up as contacts, set the CGI and object authorizations for Nagios contacts, specify the systems and services to monitor, specify display preferences for the dashboard, set up logging preferences, and set up notifications. As the Linux `root` user, you can go to the **OES Remote Manager Configuration Options > Nagios Configuration Options** in order to perform the tasks described in Table 7-2.

Table 7-2 *Nagios Configuration Options*

Nagios Configuration Option	Related File or Command	Description
Edit Nagios cgi config file	/etc/nagios/cgi.cfg	Defines the CGI parameters and which contacts or contact groups are allowed to access them.
Edit Nagios command config file	/etc/nagios/command.cfg	Defines commands, including service check, service notification, host check, host notification, service event handler, and host even handler.

Nagios Configuration Option	Related File or Command	Description
Edit Nagios config file	/etc/nagios/nagios.cfg	Specifies the main log file where service and host events are logged. For more information, see Section 7.10, “Configuring Nagios Logging,” on page 59. You can configure other Nagios parameters as defined in the configuration file.
Edit Nagios object command config file	/etc/nagios/objects/commands.cfg	Provides you with some sample command definitions that you can reference in host, service, and contact definitions.
Edit Nagios object contact config file	`/etc/nagios/objects/contacts.cfg`	By default, defines the `nagiosadmin` user as a contact and adds the contact to the contact group `admins`. You must specify an email address to use for alert notifications sent to the `nagiosadmin` contact. You can configure Nagios users as contacts and set up contact methods for each one, such as email, pager, cell phone, instant message, audio alert, and so on. You can also add a contact as a member of the default contact group `admins`, or create other contact groups and add contacts as members.
Nagios User Management	`/etc/nagios/htpasswd.users`	Create a Nagios user name and password, or delete a Nagios user. You can also use this option to create the user name with a different password. For more information, see Section 7.8, “Managing Nagios Users,” on page 56.
Restart Nagios	`rcnagios restart`	Restart the Nagios daemon after you make changes to the configuration files.

OES Remote Manager provides a text editor to modify the configuration files from the web browser. The configuration options are described in-line in each of the Nagios configuration files. After you modify the configuration files, you must restart Nagios to apply the settings. You can alternatively log in to the server as the Linux root user and use a text editor to modify the configuration files in the `/etc/nagios` folder.

After you modify the configuration files, you should verify the configuration before you restart Nagios. The Nagios daemon will not start if the configuration contains errors.

To verify your configuration, run Nagios with the -v command line option:

```
/usr/sbin/nagios -v /etc/nagios/nagios.cfg
```

If critical data is missing or wrong, Nagios displays a warning or error message that identifies the line in the configuration file that seems to be the source of the problem. Nagios might print only the first error it encounters to prevent the error from cascading the problem to subsequent settings in the file. If you get an error message, correct the line in the configuration file, then repeat the verification until no errors occur. Warning messages can generally be safely ignored, because they are recommendations and not requirements.

7.5.3 Accessing the Nagios Website

The Nagios website configuration file (`/etc/apache2/conf.d/nagios.conf`) uses basic authentication by default. Information and passwords are sent in clear text.

IMPORTANT: You should access Nagios behind the firewall or via secure channels.

When you click Nagios Service Detail, the monitoring dashboard opens in a pop-up browser window. If the pop-up blocker is enabled for your web browser, ensure that you disable the browser's pop-up blocker for the Nagios website (http://<server_ip_address or localhost>/nagios).

Authentication is required by default. You are prompted to log in. You can log in as the default user `nagiosadmin`, or create and configure other Nagios users.

To access the Nagios Service dashboard via OES Remote Manager:

1. Log in to OES Remote Manager as the Linux root user or as a LUM-enabled administrator user.
2. Select **Diagnose > Server Health Services**.
3. Click **Nagios Service Detail**.
4. When you are prompted to authenticate by Nagios Access, specify the user name and password of a Nagios user account, then click **OK**.

To access Nagios reports via the native Nagios browser view:

1. In a web browser, go to the Nagios URL:

   ```
   http://<server_ip_address>/nagios
   ```

2. When you are prompted to authenticate by Nagios Access, specify the user name and password of a Nagios user account, then click **OK**.
3. Under **Monitoring** on the left panel of the server's Nagios home page, click **Service Detail**.

7.5.4 Using Nagios Plug-Ins

Nagios plug-ins are extensions to Nagios that allow you to monitor hosts, devices, services, protocols, and applications. A plug-in performs a specific type of check and reports the results to Nagios.

The Nagios plug-ins package (`nagios-plugins`) provides a set of basic system monitoring plug-ins. It also includes plug-in libraries that are used by the basic plug-ins and additional plug-ins. You can also find Nagios plug-ins for a variety of services and applications on the *Nagios Exchange* (http://exchange.nagios.org/) website. Currently, OES does not provide plug-ins specifically designed for OES products and services.

Novell Support for Nagios plug-ins is limited to the plug-ins provided by Novell. For information about using the Nagios basic plug-ins, see the Nagios Plug-ins Documentation (http://www.nagios-plugins.org/doc/index.html) on the Nagios Plug-Ins Project (http://www.nagios-plugins.org/) website. If you use third-party plug-ins or open source plug-ins, you must refer to the providers of those plug-ins for support.

A Nagios plug-in can be compiled binaries (written in programming languages such as C or C++) or executable scripts (such as shell, Perl, or PHP). For information about how to create your own Nagios plug-ins, see the **Nagios Plug-in Development Guidelines** (http://www.nagios-plugins.org/doc/index.html) on the Nagios Plug-Ins Project (http://www.nagios-plugins.org/) website.

7.5.5 Using Object Configuration Files

Templates for Nagios object configuration files are in the `/etc/nagios/objects` directory. When you start or restart Nagios, it caches the object definitions in the `/var/lib/nagios/objects.cache` file. The CGIs read information from the cache file, rather than directly from the object configuration files, in order to prevent inconsistencies that can occur if you modify the configuration files after Nagios starts. Thus, if you modify a configuration file, you must restart Nagios to apply the change.

7.5.6 Additional Information

For detailed information about configuring and using Nagios to monitor your server and services, see the *Nagios Documentation* (http://www.nagios.org/documentation) at Nagios.org.

For additional information about CGI permissions, see *Authentication and Authorization in the CGIs* (http://nagios.sourceforge.net/docs/3_0/cgiauth.html) in the Nagios Core documentation.

7.6 Monitoring Service Health with Nagios

The Nagios website allows you to monitor the basic services and the services that you configure Nagios to monitor.

You must set up the credentials for the `nagiosadmin` user before you can view the Nagios health website. For more information, see Section 7.5.1, “Configuring Nagios Authenticated Users and Contacts,” on page 47.

You can also configure other Nagios users. For more information, see Section 7.8, “Managing Nagios Users,” on page 56.

To monitor service health with Nagios:

1. Log in to OES Remote Manager as the Linux `root` user or as a LUM-enabled administrator user.
2. Access the Nagios Service Detail page, using any of the following methods in OES Remote Manager:
   - Click the **Overall server health status indicator** icon .
   - Click the **Health Monitor** icon in the header frame.
   - Select **Diagnose > Server Health Services**.
3. On the Nagios Service Detail page, click the **Nagios Service Details** link to view the Nagios website.
4. When you are prompted, log in to Nagios using the Nagios credentials for the `nagiosadmin` user or log in another Nagios user that you have configured as a Nagios contact.

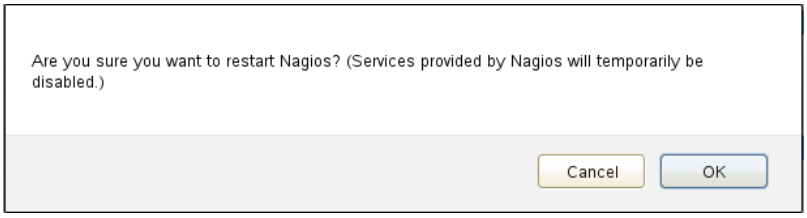
   You remain logged in to the Nagios website until you close the web browser.

   For information about setting up Nagios users, see Section 7.8, “Managing Nagios Users,” on page 56.
5. When you are done, close the web browser to log out of the Nagios website.

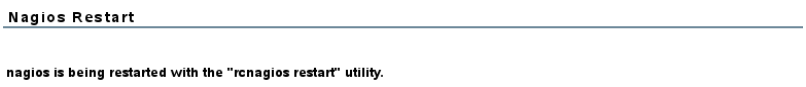
7.7 Restarting Nagios

To restart Nagios from OES Remote Manager:

1. Log in to OES Remote Manager as the Linux `root` user.
2. Click the **Configure** icon in the toolbar to go the OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Restart Nagios**.
4. When you are prompted to confirm the restart, click **OK** to proceed.



5 Wait while Nagios is restarted with the `rcnagios restart` utility.



When the restart is completed, OES Remote Manager returns to the Configuration Options page.

To restart Nagios from the command line:

1 Log in to the server as the Linux `root` user, then open a terminal console.

2 At the command prompt, enter

```
rcnagios restart
```

7.8 Managing Nagios Users

The Nagios User Management tool allows you to add and delete Nagios users, or re-create users to configure new passwords for them. Before you can access the Nagios website, you must use this tool to set a password for the Nagios user `nagiosadmin`.

- Section 7.8.1, “Creating or Re-Creating a Nagios User,” on page 56
- Section 7.8.2, “Setting Passwords for Nagios Users,” on page 57
- Section 7.8.3, “Deleting a Nagios User,” on page 57
- Section 7.8.4, “Configuring Nagios Contacts and Notification Methods for Them,” on page 57
- Section 7.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 58

7.8.1 Creating or Re-Creating a Nagios User

1 Log in to OES Remote Manager as the Linux `root` user.

2 Go to OES Remote Manager Configuration Options page.

3 Under **Nagios Configuration Options**, click **Nagios User Management**.

4 Specify the user name for a Nagios user.

5 Set the password for the Nagios user. Type a password, then type it again to confirm.

Passwords are required by default. You must set a password to ensure that authentication is required to access the Nagios web-based dashboard.

6 Click **Create User**.

The user name and password are saved in the `/etc/nagios/htpasswd.users` file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.

7 If you are creating a new Nagios user, ensure that you configure the contact information for the user and the actions the user is allowed to make. Continue with the following sections:

- Section 7.8.4, “Configuring Nagios Contacts and Notification Methods for Them,” on page 57
- Section 7.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 58

7.8.2 Setting Passwords for Nagios Users

You typically set passwords for Nagios users when you create the user names.

To add or modify a password for an existing Nagios user:

1. Log in to OES Remote Manager as the Linux `root` user.
2. Go the OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Nagios User Management**.
4. Specify the user name for an existing Nagios user.
5. Set the password for the user. Type a password, then type it again to confirm.
6. Click **Create User**.

   The user name and password are saved in the `/etc/nagios/htpasswd.users` file. The password is stored in encrypted format. The password is enforced on the next login to Nagios.

7.8.3 Deleting a Nagios User

Only Nagios users are allowed to access the web-based Nagios dashboard. Do not delete the Nagios user name of a Nagios contact who needs access to the dashboard.

IMPORTANT: Do not delete the default Nagios user `nagiosadmin`.

---

1. Log in to OES Remote Manager as the Linux `root` user.
2. Click the **Configure** icon in the toolbar to go to the OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Nagios User Management**.
4. Specify the user name for an existing Nagios user.
5. Ignore the **Password** and **Confirm Password** fields.
6. Click **Delete User**.

   The user name and password are removed from the `/etc/nagios/htpasswd.users` file. The access is denied on the user's next login to Nagios.

7.8.4 Configuring Nagios Contacts and Notification Methods for Them

After you create a Nagios user, you should define the user as a Nagios contact, in order to control what that user is allowed to do and see. Define the contact in the Nagios Object Contact configuration file on the OES Remote Manager Configuration Options page (or in the `/etc/nagios/objects/contacts.cfg` file). You can use the `nagiosadmin` definition as a template. You must restart Nagios to apply the changes.

To define a new contact:

1. Log in to OES Remote Manager as the Linux `root` user.
2. Click the **Configure** icon to go to the OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Nagios User Management**, then create a user name and password for the user.

For more information, see Section 7.8, “Managing Nagios Users,” on page 56.

4 Under **Nagios Configuration Options**, click **Edit Nagios Object Contact configuration**.

5 Add a contact definition for the existing user name, and provide a valid email address where you want to receive alert notifications for the user.

6 (Optional) Add other contact methods to the contact definition, such as pager, cell phone, instant message, audio alert, and so on.

7 (Optional) Add the contact name as a member of the contact group `admins`, or to another contact group that you have defined.

8 Under the editing window, click **Save Changes**.

9 Configure the contact or the contact group for CGI access.

For more information, see Section 7.8.5, “Configuring Nagios CGI Authorization for Contacts,” on page 58.

10 Under **Nagios Configuration Options**, click **Restart Nagios** to apply the changes.

7.8.5 Configuring Nagios CGI Authorization for Contacts

The Nagios CGI settings determine who has access to view monitoring and configuration information, and who can submit commands to the Nagios daemon through the web interface. By default, in the CGI configuration file (`/etc/nagios/cgi.cfg`), the Nagios contact `nagiosadmin` has all the necessary authorizations to manage and use Nagios:

- System and process information
- Configuration information
- System and process commands via the Nagios command CGI file (`/usr/lib/nagios/cgi/cmd.cgi`)
- All hosts information
- All services information
- All host-related commands via the Nagios command CGI file (`/usr/lib/nagios/cgi/cmd.cgi`)
- All service-related commands via the Nagios command CGI file (`/usr/lib/nagios/cgi/cmd.cgi`)

You can configure a Nagios contact's authorization settings in the Nagios CGI configuration file on the OES Remote Manager Configuration Options page (or in the `/etc/nagios/cgi.cfg` file). The configuration options are described in-line in the configuration file. You must restart Nagios to apply the changes.

7.9 Modifying the Nagios Notification Methods for Contacts

The Nagios notifications system is configured by default to send email notifications to the Nagios contact `nagiosadmin`. You must set the email address to use for `nagiosadmin` in the Nagios Object Contact configuration file on the OES Remote Manager Configuration Options page (or in the

/etc/nagios/objects/contacts.cfg file). You must restart Nagios to apply the changes. For more information, see "Setting or Modifying an Email Address for the nagiosadmin Contact" on page 49.

If you define other Nagios contacts, you must specify at least one notification method for the contact. In addition to email, Nagios can send notifications via pager, cell phone, instant message, audio alert, and so on. How notifications are sent depends on the notification commands that are defined in your object definition files.

Each host and service definition has a contact_groups option that specifies which contact groups receive notifications for that particular host or service. Contact groups can contain one or more individual contacts. Each member contact receives alert notifications according the method configured in its contact definition.

To configure the notification methods to use for Nagios contacts:

1. Log in to OES Remote Manager as the Linux root user.
2. Go to OES Remote Manager Configuration Options page.
3. Under **Nagios Configuration Options**, click **Edit Nagios Object Contact configuration**.
4. In each contact definition, use the email parameter to specify a valid email address where you want to receive alert notifications that are sent to them. For example, bob@example.com.

   You can use other notification parameters in a contact definition to specify alternative notification methods for the contact.
5. Under the editing window, click **Save Changes**.
6. Under **Nagios Configuration Options**, click **Restart Nagios** to apply the changes.

7.10 Configuring Nagios Logging

By default, Nagios logs events for the host and services in the /var/log/nagios/nagios.log file. Use the /etc/nagios/nagios.cfg file to control logging for Nagios. For information about logging options, see Table 7-3.

Table 7-3 *Nagios Logging Options*

Logging Parameter	Description and Logging Options	Default Setting
log_file	Specifies the path of the log file, including the file name.	/var/log/nagios/nagios.log

Logging Parameter	Description and Logging Options	Default Setting
`log_rotation_method`	Specifies the rotation method that Nagios should use to rotate its main log file, or disables rotation of the log. ◆ **n:** None, don't rotate the log ◆ **h:** Hourly rotation (at the top of the hour, every hour) ◆ **d:** Daily rotation (at midnight, every day) ◆ **w:** Weekly rotation (at midnight on Saturday evening) ◆ **m:** Monthly rotation (at midnight on the evening of the last day of the month)	Rotate the `nagios.log` file at midnight every day.
`log_archive_path`	Specifies the path of the directory where rotated (archived) log files are stored, if log rotation is enabled.	`/var/log/nagios/archives`
`use_syslog`	Specifies whether to log Nagios messages to the syslog facility as well as to the Nagios main log file. ◆ **1:** Enable messages to syslog. ◆ **0:** Disable messages to syslog.	Messages are sent to syslog as well as to `nagios.log`.
`log_notifications`	Specifies whether to log notifications. ◆ **1:** Log notifications. ◆ **0:** Do not log notifications.	Log notifications.
`log_service_retries`	Specifies whether to log service check retries. ◆ **1:** Log service check retries. ◆ **0:** Do not log service check retries.	Log service retries.
`log_host_retries`	Specifies whether to log host check retries. ◆ **1:** Log host check retries. ◆ **0:** Do not log host check retries.	Log host check retries.
`log_event_handlers`	Specifies whether to log host and service event handlers. ◆ **1:** Log host and service event handlers. ◆ **0:** Do not log host and service event handlers.	Log host and service event handlers.

Logging Parameter	Description and Logging Options	Default Setting
log_initial_states	Specifies whether to log the initial state for every host and service the first time its status is checked. Enable this option only if you are using an external application that reports its long-term state statistics. ◆ **1:** Log the initial state for every host and service. ◆ **0:** Do not log the initial state for every host and service.	Do not log the initial state for every host and service.
log_external_commands	Specifies whether to log external commands. ◆ **1:** Log external commands. ◆ **0:** Do not log external commands. **NOTE:** The check_external_commands option is enabled by default for OES Remote Manager. This enables you to use the CGI command interface. The command_check_interval is set to -1 by default for OES Remote Manager. This causes Nagios to check the external command file as often as possible.	Log external commands.
log_passive_checks	Specifies whether to log passive host and service checks. ◆ **1:** Log passive checks. ◆ **0:** Do not log passive checks.	Log passive checks.

7.11 Viewing the PIDs or Monitoring the Health of Processes

To view process information, click **Manage Linux > View Process Information**. On the Process Information page, you can view a list of active processes. Table 7-4 describes the health information that is reported for each process:

Table 7-4 *Process Health Information*

Parameter	Description
Process Information	Shows an **Information** icon. Click the **Information** icon next to the process name to monitor or kill an individual process.
Name	Shows the process or executable program name.
Owner	Shows the process owner (the user who started the process).

Parameter	Description
ID (Status)	Shows the process ID (PID) of the task and the current state of the task. The states are Sleep (S), Running (R), Traced (T), or Zombied (Z). These states are modified by a trailing character as follows: ◆ < indicates a process with a negative nice value. ◆ N indicates a process with a positive nice value. ◆ W indicates a swapped-out process for non-kernel processes.
CPU Usage %	Shows the task's share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.
Priority	Shows the priority of the task.
Run Time	Shows the total CPU time that the task has used since it started.
Physical Memory (%)	Shows the amount of physical memory in bytes that the task is using, and the percentage of RAM memory that this represents. The Linux `top` command reports this information in kilobytes.
Virtual Memory	Shows the amount of virtual memory in bytes that the task is using to hold the code, data, and stack space memory. This is the value reported by the Linux `top` command's RSS switch. The Linux `top` command reports this information in kilobytes.

7.12 Monitoring or Killing an Individual Process

On the Process Information page for a selected process, you can view information about the process; issue a SIGTERM, SIGKILL, or SIGHUP signal to kill the process; or send a custom signal. The process information is obtained from the `stat` file that is available for the process ID in the `/proc` directory. Process information can also be retrieved at the command line by using the Linux `top` command.

To view process information, click **Manage Linux > View Process Information**, then click the name link of the process.

Table 7-5 *Process Information*

Parameter	Description
Process Name	Shows the process or executable program name.
Process ID	Shows the process identifier.
Status	Shows the current status of the process. The status can be running, sleeping (an interruptible wait), zombie, D (waiting in uninterruptible disk sleep), T (traced or stopped on a signal), or W for paging.
Command Line	Shows the actual command line of the executed command to start this process.
Working Directory	Shows the current working directory of the process.
Executable Path	Shows the actual path name of the executed command to start this process.
Total Memory	Shows the total memory allocated to this process.

Parameter	Description
Code Size	Shows the total memory allocated for code to this process.
Data Size	Shows the total memory allocated for data to this process.
Library Memory	Shows the total memory allocated for libraries to this process.
Dirty Pages	Shows the total memory that is dirty that belongs to this process.
Resident Pages	Shows the amount of memory that this process is using that has not been swapped out.
Tasks	Shows a list of tasks or threads belonging to this process.
File Descriptors	Shows a list of file descriptors that the process has open.

7.13 Troubleshooting a Suspect or Bad Health Status

When the health status of an item changes from good to a suspect or bad state, you can look at the specific item and check the online help for suggested remedies.

1. In OES Remote Manager, access **Server Health Services**.
2. Look for the specific health service that has changed status.
3. View the information of the service that has changed by clicking the service link.

   It displays the Service State Information of the specific service.

8 Viewing File Systems

The **Home** icon and **View File System** section in OES Remote Manager for Linux include the following links to these pages:

Table 8-1 *Links for Viewing File System Information*

Link	Page Displayed
Home icon	File System Management
View File System Listing	Directory Listing of / (`root`) directory
View Partition Information	Partition Information

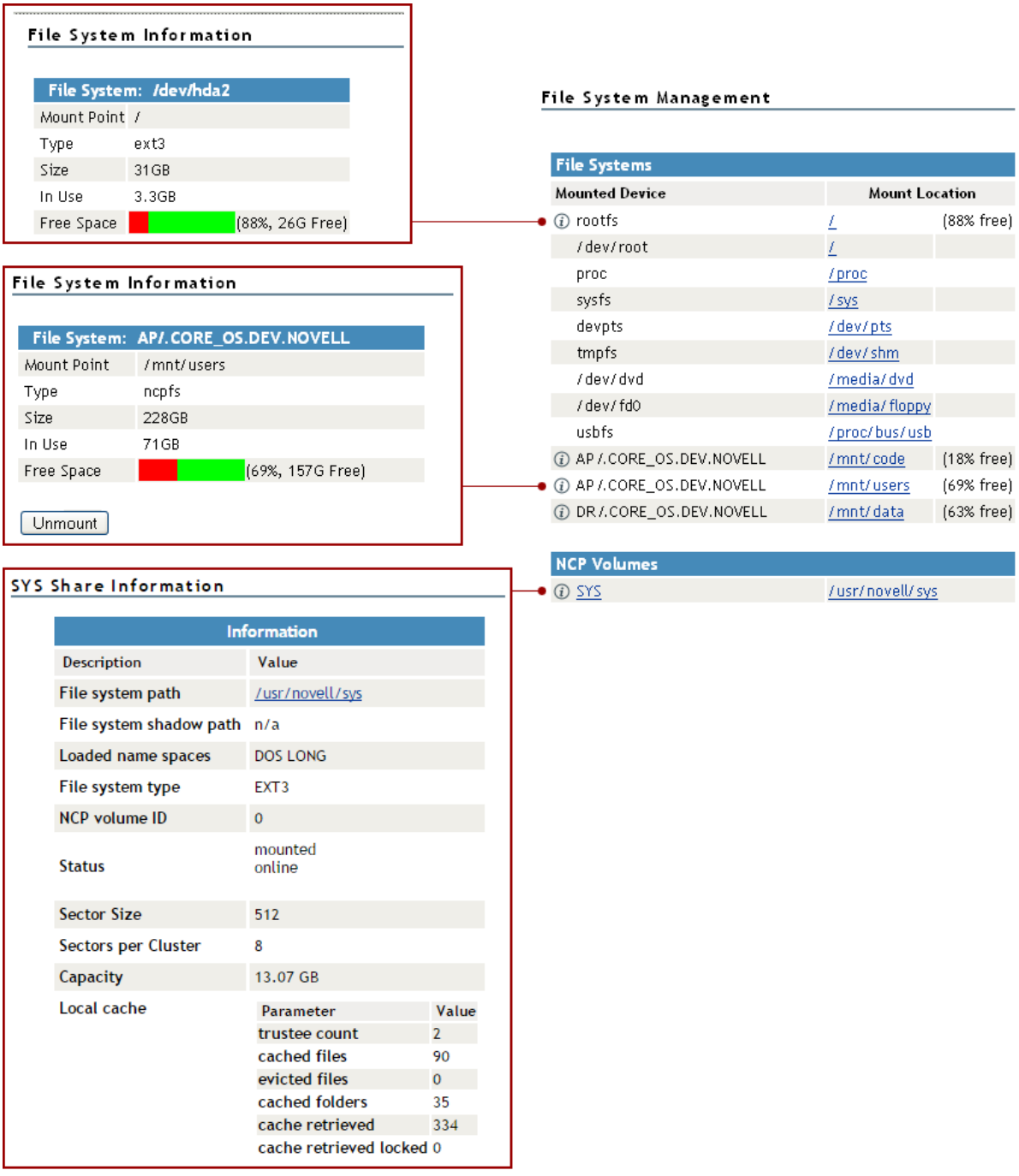
From these pages you can perform the following tasks:

- Section 8.1, “Viewing Mounted Devices and Performing Actions on Them,” on page 66
- Section 8.2, “Browsing File Systems and Performing Actions on Them,” on page 67
- Section 8.3, “Viewing Partition Information,” on page 72

8.1 Viewing Mounted Devices and Performing Actions on Them

The File System Management page is the home page for OES Remote Manager.

Figure 8-1 *File System Management Page with Information Pages*



You can access this page by clicking the Home icon (File System) link in the header frame.

The File System Management page provides a list of the server's mounted devices. The devices that are shown are from the Linux mountable file, which is a list of other file systems mounted on this host's file system.

You can view the percent of free space available on all mounted physical devices or external file systems that have actual disk space. Available disk space on virtual file systems is not shown. For information about how NSS reports space usage for volumes, see "Guidelines for Sizing Volumes" in the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

To view specific information about each mounted physical device or external file system that has actual disk space, click the **Information** icon ⓘ on the left. Clicking the **Information** icon displays one of the following types of pages:

- **File System Information.** This page shows the mount point, the file system type, the size of the mount point and the space in use. Clicking the **Unmount** button on this page, dismounts the remote file system shown. The **Unmount** button is available only on remotely mounted file systems such as NFS, NCP, and Samba.
- **NCP Share Information.** This page shows the volumes underlying file system type, mount point and status, and cache information.

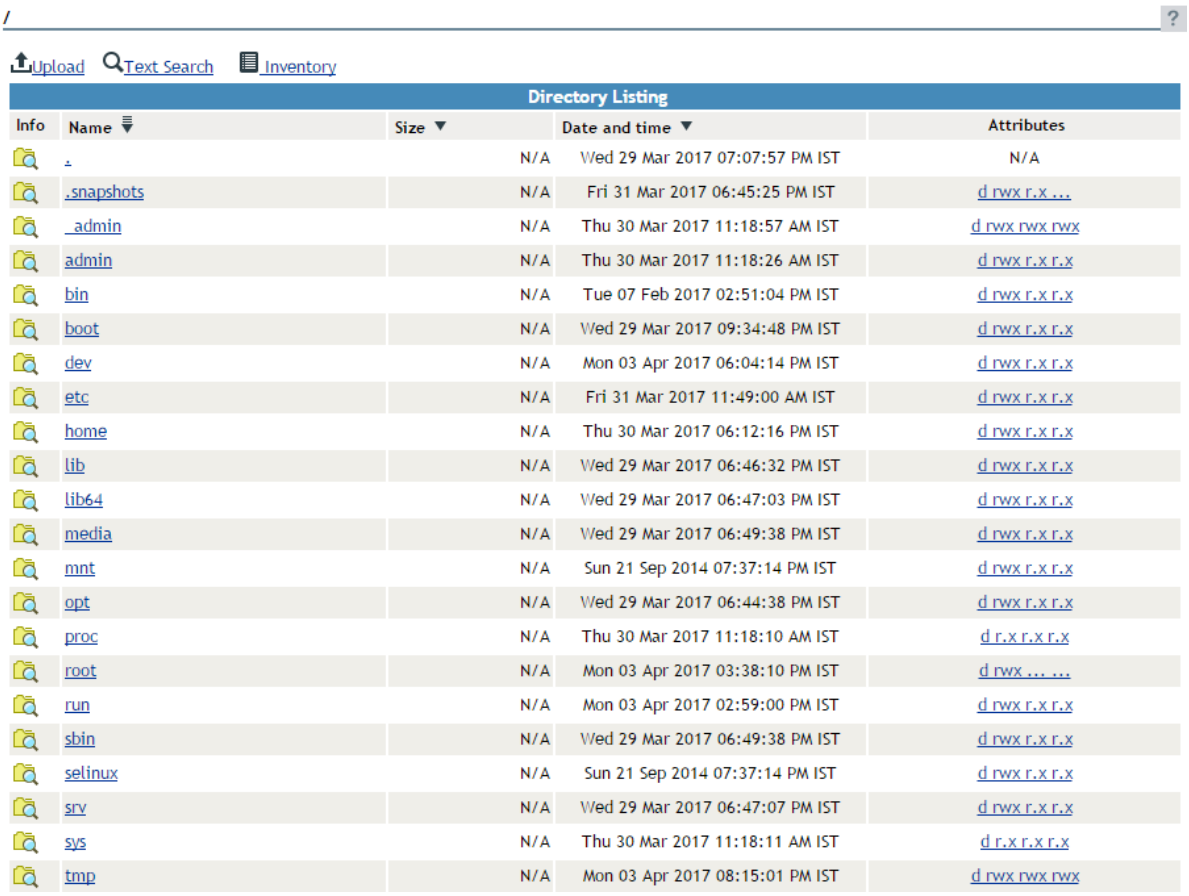
You can browse any of these file systems by clicking the link in the **Mount Location** column. At this point, you can perform any of the tasks listed for browsing the servers file system. See "Browsing File Systems and Performing Actions on Them" on page 67.

8.2 Browsing File Systems and Performing Actions on Them

On the Directory List page, you can view the Linux POSIX file system and NSS file system from mount points or local partitions; browse directories and files; view and change attributes, directories, and files; and edit, delete, or rename files.

To access this page, click **View File System** > **View File System Listing** in the navigation frame.

Figure 8-2 *Directory List Page*


/
Upload
Text Search
Inventory
Directory Listing
Info
Name
Size
Date and time
Attributes
. N/A Wed 29 Mar 2017 07:07:57 PM IST N/A
.snapshots N/A Fri 31 Mar 2017 06:45:25 PM IST d rwx r.x ...
_admin N/A Thu 30 Mar 2017 11:18:57 AM IST d rwx rwx rwx
admin N/A Thu 30 Mar 2017 11:18:26 AM IST d rwx r.x r.x
bin N/A Tue 07 Feb 2017 02:51:04 PM IST d rwx r.x r.x
boot N/A Wed 29 Mar 2017 09:34:48 PM IST d rwx r.x r.x
dev N/A Mon 03 Apr 2017 06:04:14 PM IST d rwx r.x r.x
etc N/A Fri 31 Mar 2017 11:49:00 AM IST d rwx r.x r.x
home N/A Thu 30 Mar 2017 06:12:16 PM IST d rwx r.x r.x
lib N/A Wed 29 Mar 2017 06:46:32 PM IST d rwx r.x r.x
lib64 N/A Wed 29 Mar 2017 06:47:03 PM IST d rwx r.x r.x
media N/A Wed 29 Mar 2017 06:49:38 PM IST d rwx r.x r.x
mnt N/A Sun 21 Sep 2014 07:37:14 PM IST d rwx r.x r.x
opt N/A Wed 29 Mar 2017 06:44:38 PM IST d rwx r.x r.x
proc N/A Thu 30 Mar 2017 11:18:10 AM IST d r.x r.x r.x
root N/A Mon 03 Apr 2017 03:38:10 PM IST d rwx ... ...
run N/A Mon 03 Apr 2017 02:59:00 PM IST d rwx r.x r.x
sbin N/A Wed 29 Mar 2017 06:49:38 PM IST d rwx r.x r.x
selinux N/A Sun 21 Sep 2014 07:37:14 PM IST d rwx r.x r.x
srv N/A Wed 29 Mar 2017 06:47:07 PM IST d rwx r.x r.x
sys N/A Thu 30 Mar 2017 11:18:11 AM IST d r.x r.x r.x
tmp N/A Mon 03 Apr 2017 08:15:01 PM IST d rwx rwx rwx

The following table describes the actions necessary to access directories, files, and file and directory attributes from the Directory List page.

Table 8-2 *Directory List Page Tasks and Procedures*

Tasks	Procedures
Browse to a mount point, volume, directory, or local partition	Click the *link_for_the_mount_point*, *volume*, *directory*, or *local partition* under the **Name** column.
Move down the directory tree	Click the *directory_name* link.
Move up the directory tree	Click the *double_dots* (..) link.
Re-sort the list by name, size, or date and time.	Click the *column heading* that has a **Sort** icon next to it. The default sort for this listing is by the directory or file name.
View or change the attributes of a directory	Click the **Attributes** link. For information, see Section 8.2.1, "Viewing or Changing File or Directory Attributes," on page 69.
View the size of a directory or file.	The **Size** column for a directory lists the size of all files and subdirectories in that directory.

From the Directory Listing page, you can perform the following tasks.

- Section 8.2.1, “Viewing or Changing File or Directory Attributes,” on page 69
- Section 8.2.2, “Viewing Details about Directories and Performing Actions on Them,” on page 69
- Section 8.2.3, “Uploading a File to the Server,” on page 70
- Section 8.2.4, “Downloading a File from the Server to a Local Workstation,” on page 70
- Section 8.2.5, “Searching for Text in Files,” on page 71
- Section 8.2.6, “Viewing the Details of a File and Performing Specific Actions,” on page 71
- Section 8.2.7, “Viewing Individual Files,” on page 72

8.2.1 Viewing or Changing File or Directory Attributes

Clicking the **Attributes** link opens the Directory Information page where you can view or change the attributes of the directory. For more information, see “Viewing Details about Directories and Performing Actions on Them” on page 69 and “Viewing the Details of a File and Performing Specific Actions” on page 71.

IMPORTANT: To set directory and file attributes for files on the NSS file system, go to **Manage NCP Services > Manage Shares**, the browse to locate the file and set its attributes. You can also use iManager, Client for Open Enterprise Server, or OES NetStorage.

Viewing attributes on NSS volumes, directories, and files conveys the status of the NSS file system directory and file attributes: Hidden (H), Read Only (Ro), Read/Write (Rw), and Execute (X). You can view these settings in OES Remote Manager for Linux as a combination of Read, Write, and Execute fields for the User, Group, and Other categories. Although it appears that you can control these attributes using the selections on the Directory Information page, the selections do not actually control the conventional POSIX settings for NSS directories and files. For more information, see “Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions” in the *OES 2018: File Systems Management Guide*.

8.2.2 Viewing Details about Directories and Performing Actions on Them

1. Click the **View File System** > **View File System Listing** link in the navigation frame or click a *Mount_Location_name* link on the **Home** page.
2. On the Directory list page, browse to the directory you want to search in by clicking the *directory_name* link.
3. From the directory listing, click the **Folder Information** icon to the left of the directory or subdirectory you want to view information about or change the attributes of.
4. On the Directory Information page that is displayed, view the information or select/deselect the check box for the attributes that you want to change.
5. Click **OK**.
6. When viewing the details of a directory from the Directory Information page, you can also perform the following tasks for the selected directory:
   - Delete the directory and its contents

- Rename the directory
- Create a subdirectory in the directory
- Create a symbolic link in the directory

Type the required information in the field next to the option, then click its button.

8.2.3 Uploading a File to the Server

If you have rights to write to the current directory that you are viewing via OES Remote Manager, you can use the **Upload** link to copy a file from your local machine or any other network directory to the currently selected directory.

You can upload only one file at a time. The file's date and time are changed when performing this task.

To perform this task:

1. Click the **View File System** > **View File System Listing** link in the navigation frame or click a *Mount_Location_name* link on the **Home** page.
2. On the Directory list page, browse to the directory you want to upload a file to by clicking the *directory_name* link.
3. In the directory listing, click the **Upload** link at the top of the Directory listing page.
4. Browse to and select the file that you want to upload.
5. Click **Upload**.

8.2.4 Downloading a File from the Server to a Local Workstation

When you are browsing the server's file system via OES Remote Manager, you can download any file to your local machine by clicking the file name, and then saving the file to your local workstation.

1. Click the **View File System** > **View File System Listing** link in the navigation frame, or click a *Mount_Location_name* link on the **Home** page.
2. On the Directory/File List page, browse to or search for the file that you want to download.
3. Click the *file_name* link.
4. When prompted, save the target file to the desired location.

   If the file opens rather than prompting you to save it, you can use the browser features to save the file.

8.2.5 Searching for Text in Files

On the Directory Listing page, you can do a GREP-type search (it accepts GREP wildcard characters) through the files in the current directory as well as subdirectories to find text in a file.

1. Click the **View File System** > **View File System Listing** link in the navigation frame or click a *Mount_Location_name* link on the **Home** page.
2. On the Directory list page, browse to the directory you want to search in by clicking the *directory_name* link.
3. Click the **Text Search** link.
4. Specify the content, file name, or extension you want to search for and select whether you want to match the case.
5. (Optional) If you want to search all subdirectories as well, select **Search Subdirectories**.
6. Click **Search**.

   If nothing is found, no files are listed under the search instructions.

   If the search instructions are not valid, the page showing the directory you wanted to search is returned.

   If the search instructions are valid, the results are displayed on a page with the search instructions.

   In the display results, you can

   - Click the file name link to view or download the file.
   - Click the **File Information** icon to view information about the file; change the attributes to it; or edit (conditional), rename, or delete the file.

     If the file is a simple text file or a file with an extension listed in the `/opt/novell/nrm/nrmedit.txt` file, you can also edit the file by clicking the **Edit File** button.

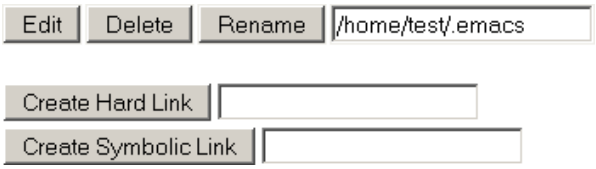
8.2.6 Viewing the Details of a File and Performing Specific Actions

1. Click the **View File System Listing** link in the navigation frame or click a **Mount Location** name link on the Home page.
2. On the Directory list page, browse the directories to the file, then click the **File** icon to the left of the file name.
3. On the File Information page that is displayed, view the information or specify the information required for the applicable task, and then click the applicable button for the task you want to perform.

   For Attributes management, click the attributes that you want to select/deselect and then click **OK**.

   For file management, use the **Edit**, **Delete**, or **Rename** buttons. The **Edit** button is available only on simple text files or files with the extensions listed in the `/opt/novell/nrm/nrmedit.txt` file.

If you want to save the file with an ANSI or UTF-8 encoding, select the appropriate option and click **OK**.



8.2.7 Viewing Individual Files

If your browser is set up to recognize a certain file extension (for example, `.txt`), you can browse to and click a file of that type to view it directly in OES Remote Manager. Otherwise, you can download any file to your local machine by clicking the file name, and then saving it to a local workstation and opening it there. See Section 8.2.4, “Downloading a File from the Server to a Local Workstation,” on page 70.

8.3 Viewing Partition Information

If you need to get information about how a partition is laid out, you can get this information from the Partition Information page. This page shows you the major and minor numbers of the partition, the number of blocks in the partition, and its name.

To view partition information, click **View Partition Information** in the navigation frame.

Figure 8-3 *Example Partition Information Page*

Partition Information

Partition Information			
major	minor	#block	name
3	0	39121488	hda
3	1	2096451	hda1
3	2	4096575	hda2
3	3	1	hda3
3	5	1052226	hda5
3	6	31872928	hda6

9 Managing Linux

The Manage Linux section in OES Remote Manager (NRM) for Linux includes the following links to these pages from which you can perform the following tasks:

Table 9-1 *Manage Linux Section Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Info, See
Access VNC Console screens	**VNC Consoles**	VNC Consoles Screens	"Accessing VNC Consoles" on page 73
View Kernel Modules Information	**View Kernel Modules**	Kernel Module Listing	"Viewing Kernel Modules" on page 75
Shut down and restart the host	**Down/Restart**	Down/Reset Options	"Shutting Down and Restarting the Host" on page 76
Manage packages	**View Package Information**	Package Information	"Managing Packages" on page 77
Manage processes	**View Process Information**	Process Information	"Managing Processes" on page 79
Schedule cron jobs to run	**Schedule Task**	Schedule Task	"Scheduling cron Jobs to Run on the Server" on page 80

9.1 Accessing VNC Consoles

If VNC services are configured on the server, you can access the VNC consoles screens in OES Remote Manager. The accessibility to the VNC consoles via OES Remote Manager for Linux is limited to user `root`; it is not available to user Admin. This form of remote administration is less secure that SSH; therefore, we recommend using this feature only in a secure environment (behind a firewall).

IMPORTANT: VNC access is disabled by default to prevent cross-site scripting. You must disable the HttpOnly setting in the `/etc/opt/novell/httpstkd.conf` file in order to enable the VNC console display. For information, see Section A.4, "HttpOnly Command," on page 161.

1 If VNC services are not configured on the server, you can configure them as follows:

   1a In **YaST**, log in as the `root` user, then click **Network Services** > **Remote Administration**.

   1b On the Remote Administration page, select the following options:

   - **Allow Remote Administration**
   - **Open Port in Firewall** (default port is 5801)

   1c Click **Finish**.

1d Restart the display manager by entering the following command at the command line:

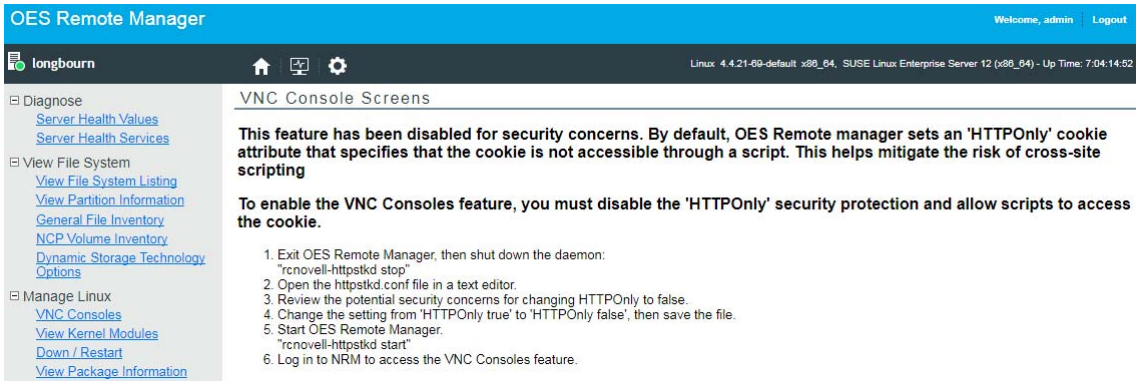
```
rcxdm restart
```

2 Verify that pop-up blocking is disabled in your web browser.

3 Log in to OES Remote Manager as the `root` user.

4 Select **Manage Linux > VNC Consoles**.

5 If VNC Consoles is disabled, a message is displayed instead of the console. You must disable the HttpOnly setting in the `/etc/opt/novell/httpstkd.conf` file in order to enable the VNC console display. For information, see Section A.4, “HttpOnly Command,” on page 161.


OES Remote Manager
Welcome, admin
Logout
longbourn
Linux 4.4.21-69-default x86_64, SUSE Linux Enterprise Server 12 (x86_64) - Up Time: 7:04:14:52
Diagnose
Server Health Values
Server Health Services
View File System
View File System Listing
View Partition Information
General File Inventory
NCP Volume Inventory
Dynamic Storage Technology Options
Manage Linux
VNC Consoles
View Kernel Modules
Down / Restart
View Package Information
VNC Console Screens
This feature has been disabled for security concerns. By default, OES Remote manager sets an 'HTTPOnly' cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting
To enable the VNC Consoles feature, you must disable the 'HTTPOnly' security protection and allow scripts to access the cookie.
1. Exit OES Remote Manager, then shut down the daemon:
"rcnovell-httpstkd stop"
2. Open the httpstkd.conf file in a text editor.
3. Review the potential security concerns for changing HTTPOnly to false.
4. Change the setting from 'HTTPOnly true' to 'HTTPOnly false', then save the file.
5. Start OES Remote Manager.
"rcnovell-httpstkd start"
6. Log in to NRM to access the VNC Consoles feature.

6 Click the **1024 X 728** button on the VNC Console Screens page.

Clicking the **VNC Consoles** link opens a Java applet in a secondary browser window. The following table explains what you can do from this window.

Table 9-2 *VNC Console Page Tasks and Procedures*

Task	Procedure
Use any of the screens listed as though you were at the server console.	Use the keyboard or mouse as though you were at the server console.
Disconnect from the console.	Click the **Disconnect** button on this page.
Change any of the VNC client options currently selected.	Click the **Options** button.
Access the VNC client clipboard and cut or paste any commands that you might want to execute in a active terminal shell.	Click the **Clipboard** button.
Restart the server.	Click the **Send Ctrl+Alt+Del** button.
Refresh the current screen you are viewing.	Click the **Refresh** button.

Figure 9-1 illustrates a user accessing YaST on a remote server from the user’s desktop browser. To access YaST on the remote server, the user did the following:

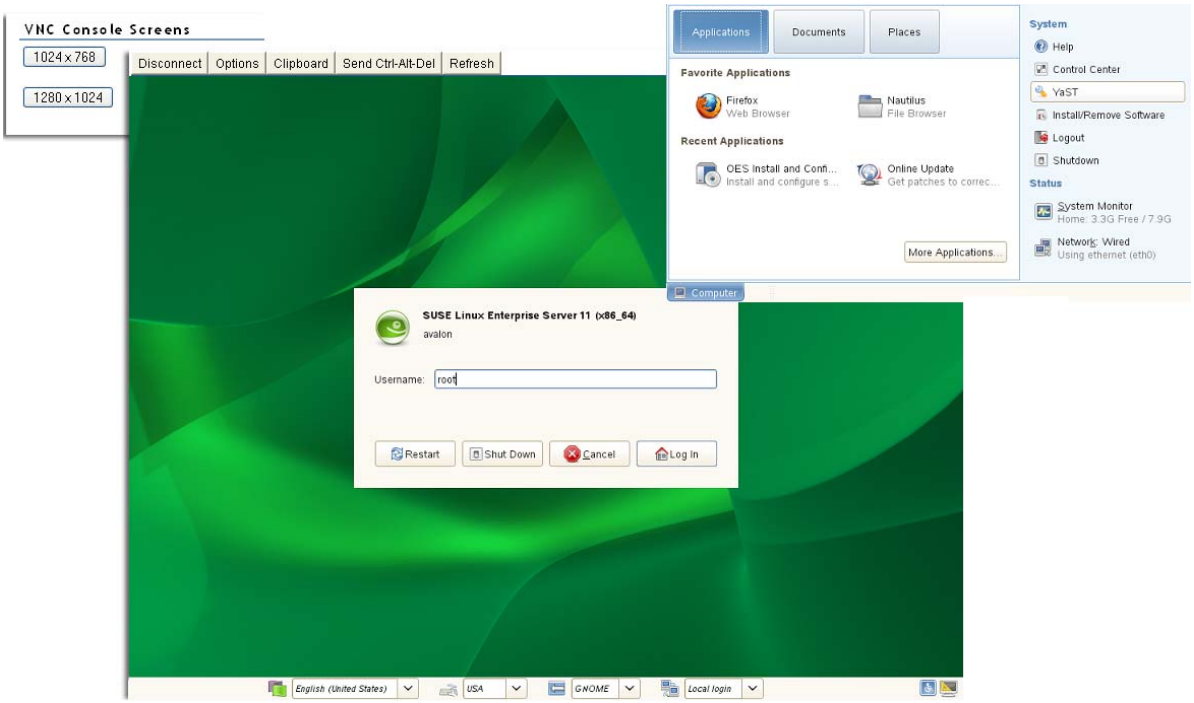
1 Clicked the **VNC Consoles** link in the navigation frame.

2 Clicked the **1024 X 728** button on the VNC Consoles Screens page.

3 Logged into Linux.

4 Clicked **Computer** > **System** > **YaST**.

Figure 9-1 *Example Access of YaST through NRM VNC Console Screens Linux on a GNOME Desktop.*

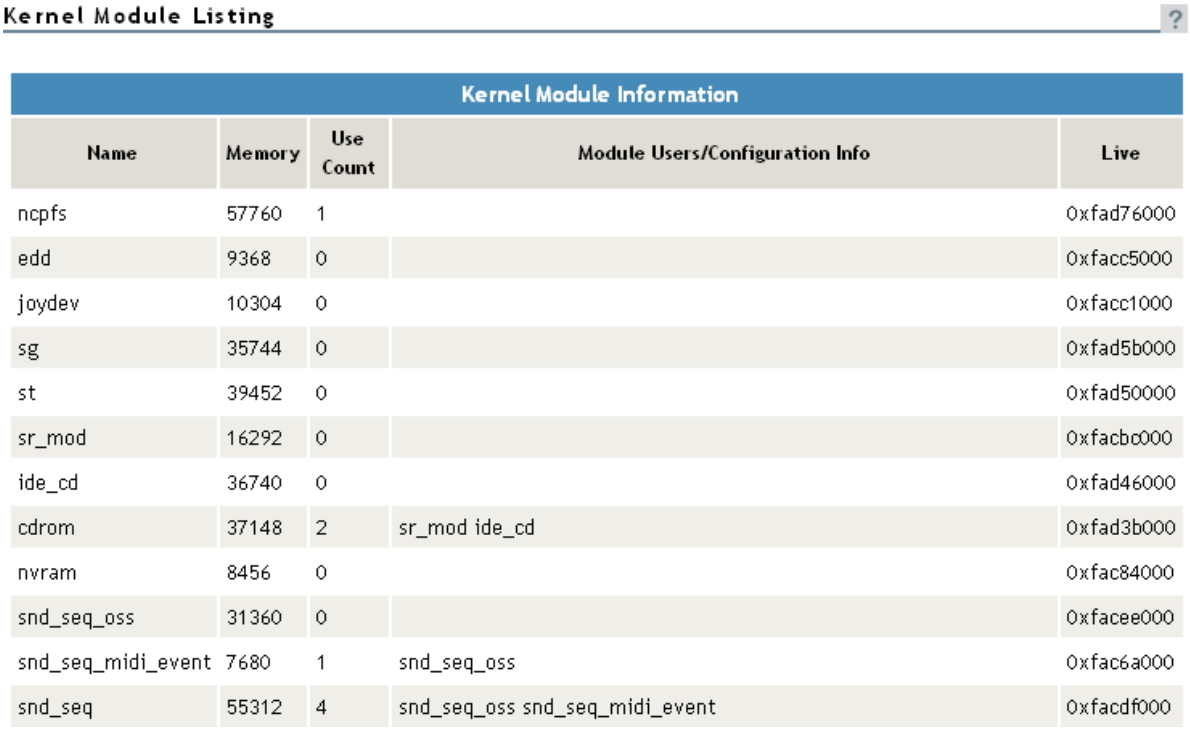


9.2 Viewing Kernel Modules

Clicking the **View Kernel Modules** link in the navigation frame displays the Kernel Module Listing page. On this page you can view the status of the modules that have been compiled into the Linux kernel on this system. Printing this page can be useful to document your system as you make changes or upgrades to it in the future.

The information shown on this page is equivalent to the information in the `lsmod` shell command plus the Live information or equivalent to viewing the `proc\modules` file.

Figure 9-2 *Example Kernel Module Listing Page*



Kernel Module Listing

Kernel Module Information				
Name	Memory	Use Count	Module Users/Configuration Info	Live
ncpfs	57760	1		0xfad76000
edd	9368	0		0xfacc5000
joydev	10304	0		0xfacc1000
sg	35744	0		0xfad5b000
st	39452	0		0xfad50000
sr_mod	16292	0		0xfacbc000
ide_cd	36740	0		0xfad46000
cdrom	37148	2	sr_mod ide_cd	0xfad3b000
nvram	8456	0		0xfac84000
snd_seq_oss	31360	0		0xfacee000
snd_seq_midi_event	7680	1	snd_seq_oss	0xfac6a000
snd_seq	55312	4	snd_seq_oss snd_seq_midi_event	0xfacdf000

9.3 Shutting Down and Restarting the Host

Clicking the **Down/Restart** link in the navigation frame displays the Down/Reset Options page. You can use these options to shut down or reset the host.

The following table describes the specific actions of each option.

Table 9-3 *Down/Reset Options Page Options and Actions*

Option	Action
Down	Forces the host to shut down immediately.
Reset	Forces the host to shut down immediately, then warm boots the computer.

Using either of the options additionally forces the host to perform the following actions:

- Update the cache buffers to disks
- Close all open files

WARNING: If files are open and changes have not been saved to the host, some data loss might occur. Users might need to save changes locally until the host is started again.

If the application that is being used to access the file creates a temporary file and locks the file, you might also need to search for and remove the temporary file.

For example, Microsoft Word creates a system file that begins with ~$, such as `~$myfile8.doc`. OpenOffice and LibreOffice create a hidden file that begins with .~lock, such as `.~lock.myfile10.odt`. You can view the temporary files by selecting **Manage Shares**, then navigating the NCP volume or NSS volume to the folder where the open file is stored.

- Update the appropriate file system tables
- Exit the host from the network
- Unmount all file systems

9.4 Managing Packages

Clicking the **View Package Information** link displays the Packing Information page. On this page you can view the following information about each package that is installed on the system:

- **Name**
- **Group**
- **Version**
- **Release**
- **Vendor**

Figure 9-3 *Example Package Information Page*

Package Information

Package Information | Install | Search | (case sensitive)

Name	Group	Version	Release	Vendor
aaa_base	System/Fhs	13.2+git20140911.61c1681	32.1	SUSE LLC
aaa_base-extras	System/Fhs	13.2+git20140911.61c1681	32.1	SUSE LLC
accountsservice	System/Daemons	0.6.42	14.2	SUSE LLC
accountsservice-lang	System/Localization	0.6.42	14.2	SUSE LLC
acl	System/Filesystems	2.2.52	6.1	SUSE LLC
adaptec-firmware	Hardware/Other	1.35	22.11	SUSE LLC
adjtimex	System/Base	1.29	3.1	SUSE LLC
adwaita-icon-theme	System/GUI/GNOME	3.20	3.2	SUSE LLC
alsa	System/Libraries	1.0.27.2	15.1	SUSE LLC
alsa-plugins	System/Libraries	1.0.27	4.74	SUSE LLC
alsa-plugins-pulse	System/Libraries	1.0.27	4.74	SUSE LLC
alsa-utils	Productivity/Multimedia/Sound/Players	1.0.27.2	9.2	SUSE LLC
ant	Development/Tools/Building	1.9.4	1.6	SUSE LLC
apache-commons-collections	Development/Libraries/Java	3.2.2	6.1	SUSE LLC
apache-commons-daemon	System/Daemons	1.0.15	6.10	SUSE LLC
apache-commons-dbcp	Development/Libraries/Java	2.1.1	2.1	SUSE LLC
apache-commons-logging	Development/Libraries/Java	1.1.3	7.1	SUSE LLC
apache-commons-pool2	Development/Libraries/Java	2.4.2	1.2	SUSE LLC
apache2	Productivity/Networking/Web/Servers	2.4.23	29.3.2	SUSE LLC
apache2-mod_php5	Productivity/Networking/Web/Servers	5.5.14	108.1	SUSE LLC
apache2-prefork	Productivity/Networking/Web/Servers	2.4.23	29.3.2	SUSE LLC
apache2-utils	Productivity/Networking/Web/Servers	2.4.23	29.3.2	SUSE LLC
apache2-worker	Productivity/Networking/Web/Servers	2.4.23	29.3.2	SUSE LLC
apparmor-docs	Documentation/Other	2.8.2	54.1	SUSE LLC
apparmor-parser	Productivity/Networking/Security	2.8.2	54.1	SUSE LLC
apparmor-profiles	Productivity/Security	2.8.2	54.1	SUSE LLC
apparmor-utils	Productivity/Security	2.8.2	54.1	SUSE LLC
appres	System/X11/Utilities	1.0.4	1.16	SUSE LLC
at	System/Daemons	3.1.14	7.3	SUSE LLC

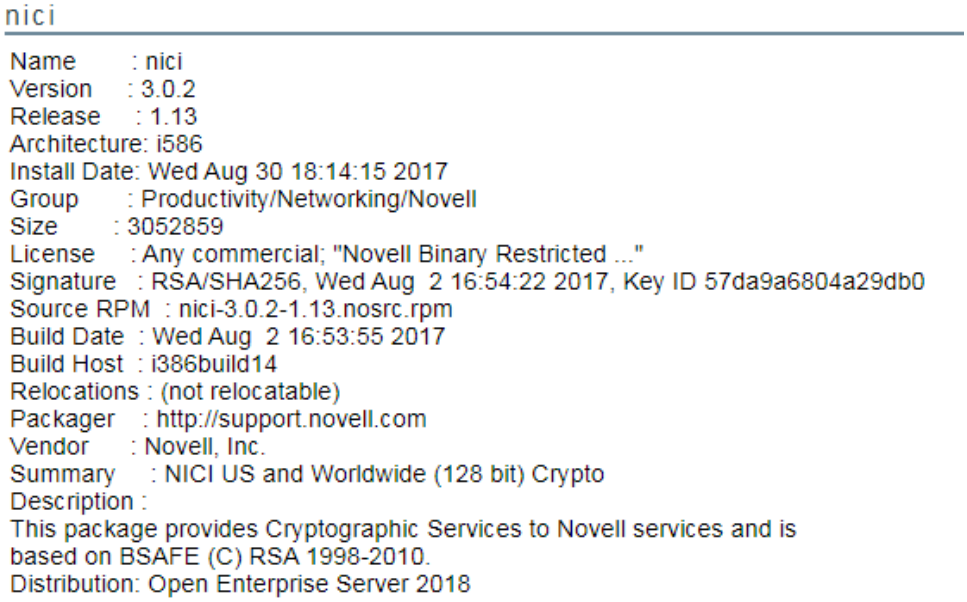
On the View Package Information page and subsequent pages, you can perform these tasks using the following procedures:

Table 9-4 *View Package Information Page Tasks and Procedures*

Tasks	Procedures
Sort the listed packages by name, group, or vendor	Click the **Sort** icon at the top of the applicable column. The default sort is by name.
View more detailed information about an installed package	Click the link for the applicable package under the **Name** column.
Remove an installed package	1. Click the *link for the package* under the Name column. 2. Click **Remove**.
Install a new package that you have downloaded to the host	1. Click **Install**. 2. Browse to the location where you uploaded the package to. The browse starts at the root of the host. 3. Click **Install**. The selected package's file path is transferred to the **RPM File Path** field on the Package Installation page. When the **Install** button is clicked on the View Package Information page, OES Remote Manager attempts to install the specified RPM file using the Linux RPM utility.

The following figure shows a sample of the details you see when you click the *package_name* link.

Figure 9-4 *Detailed Information Page for the nici Example Package*


nici
Name : nici
Version : 3.0.2
Release : 1.13
Architecture: i586
Install Date: Wed Aug 30 18:14:15 2017
Group : Productivity/Networking/Novell
Size : 3052859
License : Any commercial; "Novell Binary Restricted ..."
Signature : RSA/SHA256, Wed Aug 2 16:54:22 2017, Key ID 57da9a6804a29db0
Source RPM : nici-3.0.2-1.13.nosrc.rpm
Build Date : Wed Aug 2 16:53:55 2017
Build Host : i386build14
Relocations : (not relocatable)
Packager : http://support.novell.com
Vendor : Novell, Inc.
Summary : NICI US and Worldwide (128 bit) Crypto
Description :
This package provides Cryptographic Services to Novell services and is
based on BSAFE (C) RSA 1998-2010.
Distribution: Open Enterprise Server 2018

9.5 Managing Processes

Clicking the **View Process Information** link in the navigation frame displays the Process Information page. On this page, you can view a list of all the processes as well as their state in the host and perform the actions listed in the following table.

Table 9-5 *Process Information Page Tasks and Procedures*

Tasks	Procedures
Sort the process by name (in alphabetical order by default), by process ID, by CPU Usage, or by Memory Usage	Click the **Sort** icon ▼ at the top of the applicable column.
View more specific information about a listed process	Click the *link for t*he applicable process under the **Name** column.
Kill a process	1. Click the link for the applicable process under the **Name** column. 2. Click **Kill**.

The process information is obtained from the `stat` file that is available for each process ID in the `/proc` directory. Process information can also be retrieved at the command line by using the Linux `top` command.

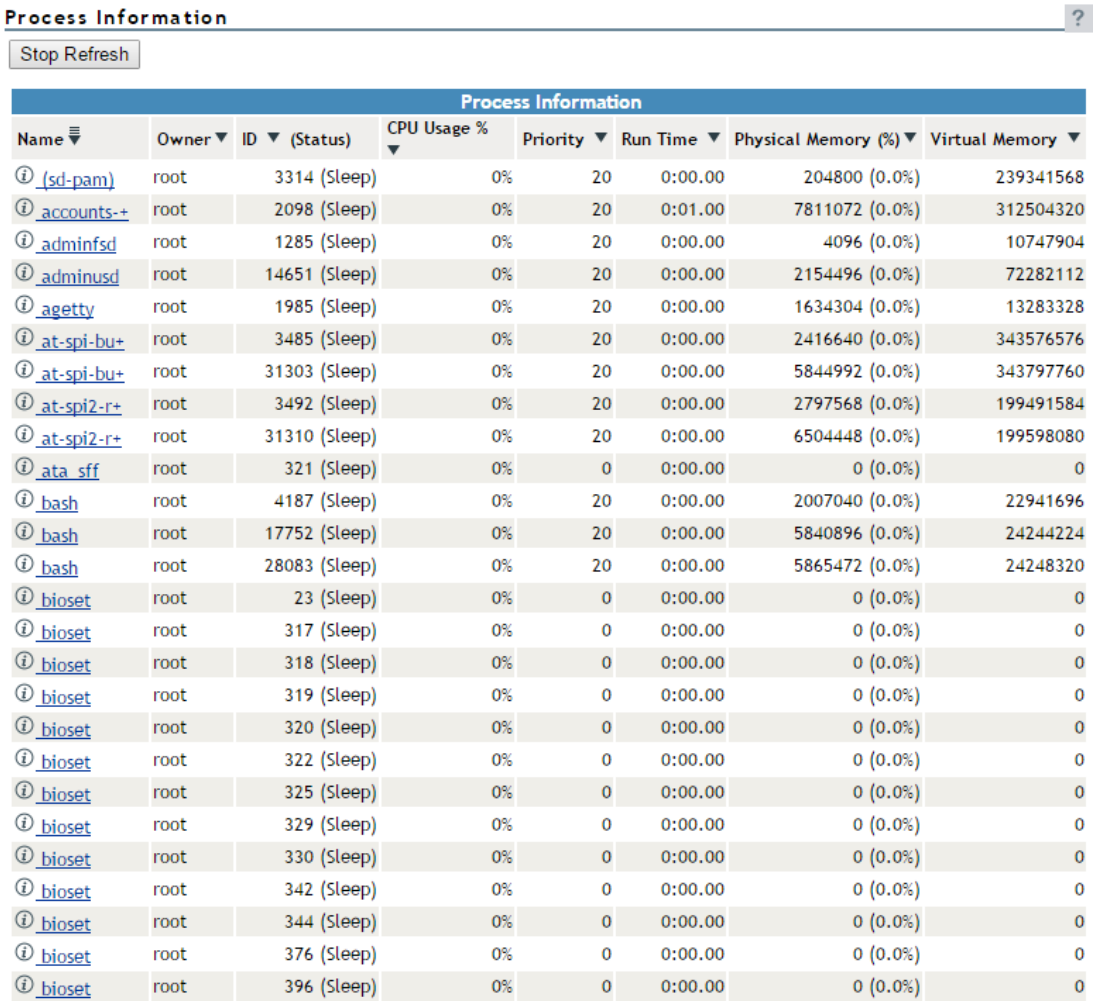
Table 9-6 on page 79 describes the parameters reported for each process.

Table 9-6 *Process Information*

Parameter	Description
Name	The process name.
Owner	The process owner; the user who started the process.
ID (Status)	The process ID of the task, and the current state of the task. The states are Sleep (S), Running (R), Traced (T), or Zombied (Z). These states are modified by a trailing < for a process with a negative nice value, N for a process with positive nice value, and W for a swapped-out process (this does not work correctly for kernel processes).
CPU Usage %	The task's share of the CPU time since the last screen update, expressed as a percentage of total CPU time per processor.
Priority	The priority of the task.
Run Time	The total CPU time the task has used since it started.
Physical Memory	The physical memory value is the amount of physical memory in bytes that the task is using. The value in parentheses (%) is the percentage of RAM memory that this represents. The Linux `top` command reports this information in kilobytes.

Parameter	Description
Virtual Memory	The virtual memory is the amount of memory in bytes that the task is using to hold the code, data, and stack space memory. The Linux `top` command reports this information in kilobytes. Virtual Memory is the value reported by the RSS switch for the top command.

Figure 9-5 *Example Process Information Page*



9.6 Scheduling cron Jobs to Run on the Server

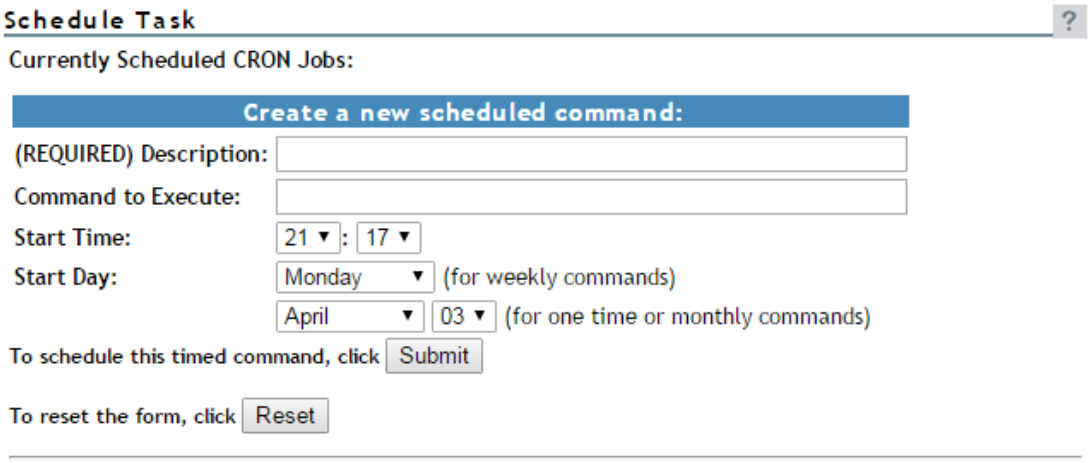
Rather than entering commands on the command line to run a cron job at a specific time, you can use a form on the Schedule Task page to schedule cron jobs—that is, to execute commands or scripts (groups of commands) automatically at a specified time/date—that you want to run at this server. Any cron job is valid.

Scheduling a task creates a cron job and stores it in the `/etc/cron.d` directory. The command is specified to run with the name of whatever user name you are logged in with when you add the command. The user name must have the necessary permissions to perform the command you add.

IMPORTANT: When you set up cron commands, you must log into OES Remote Manager as the `root` user.

If no mail service is configured, you might find the output of your commands in the local mailbox directory as a plain text file. By default, this is `/var/spool/mail/root`.

Figure 9-6 *Schedule Task Page for Scheduling Cron Jobs*



To create a new scheduled command:

1 Complete the required information on the Schedule Task page.

Field	Information to Provide
Description	Enter a brief description of the command you want to run. 64 character limit Example: Send message to log out daily at 10 p.m. This description is displayed as the name of the scheduled job in the **Currently Scheduled CRON Jobs** list.
Command to Execute	Type the command exactly as you would at a command line. All cron job entry types are valid except for lists and step values.
Start Time	Type the time you want the command to run.
Start Day	If you want to run the command once a week, specify the day of the week, then place an asterisk * in the **Month** and **Day** fields. If you want to run the command only once or monthly, specify a **Month** and **Day** setting, then place an asterisk * in the **Day of the Week** field. If you want to run the command monthly, specify a Day setting, then place an asterisk * in the **Start Day** and **Month** fields. If you do not want to specify a value for a field, place an asterisk * in the field.

2 Click **Submit**.

After you schedule a job, it is displayed at the top of the page under the **Currently Scheduled CRON Jobs** heading. Jobs that your create manually also display in the list.

To change the schedule of a job that you have already scheduled:

1 Click the link for the job you want to change.

2 Change the schedule.

3 Click **Submit**.

To delete the schedule of a job that you have already scheduled:

1 Click the link for the job you want to delete.

2 Click **Delete**.

To return the settings in the fields to the default settings of the current day and time, click **Reset**.

10 Managing Hardware

The **Manage Hardware** section in OES Remote Manager (NRM) for Linux includes the following links to pages from which you can perform the following tasks:

Table 10-1 *Manage Hardware Section Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Info, See
View Processor information	**View Processors**	Processor Information	"Viewing Processors" on page 83
View Interrupt information	**Interrupt Information**	Interrupts	"Viewing Interrupt Information" on page 84
View memory I/O information	**IO Memory Information**	I/O Memory Information	"Viewing I/O Memory Information" on page 85
View port I/O information	**IO Port Information**	IO Port Information	"Viewing I/O Port Information" on page 86
View SMBIOS information	**SMBIOS Information**	SMBIOS Information	"Viewing SMBIOS Information" on page 87

10.1 Viewing Processors

Clicking the **View Processors** link under the **Manage Hardware** heading in the navigation frame displays the Processor Information page. On this page you can view information about each processor on this host.

Information about the processor speed as well as the local cache sizes is useful in determining how much work a processor can do.

This information is equivalent to the information you would see in the `/proc/cpuinfo` file.

Figure 10-1 *Example Processor Information Page*

Processor Information

processor : 0	
vendor_id	GenuineIntel
cpu family	6
model	45
model name	Intel(R) Xeon(R) CPU E5-2440 0 @ 2.40GHz
stepping	7
microcode	1803.000000
cpu MHz	2400 .000
flags	fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts mmx fxsr sse sse2 ss ht syscall nx rdtscp lm constant

In a virtualized environment, the processor information is reported from the perspective of the server where you connected.

- **Host Server:** When you connect to OES Remote Manager by using the host server IP address, the report contains information about all processors on the system.
- **Guest Server:** When you connect to OES Remote Manager by using the guest server IP address, the report contains information about the physical hardware in use, but only for the number of processors you assign to the virtual machine.

  The guest server reports the same information about a processor as if it owned the actual hardware on the server. The Virtual Machine Monitor component of the virtualization software emulates a complete hardware environment in the virtual machine for the guest server. The guest server OS is unaware that it shares the hardware resources with other virtual machines and the host.

The actual usage statistics of the physical processors are not known by OES Remote Manager. You could use the Virtual Machine Manager to see that type of information.

10.2 Viewing Interrupt Information

Clicking the **Interrupt Information** link under the **Manage Hardware** heading in the navigation frame displays the Interrupts page, which includes the following:

Table 10-2 *Interrupts Page*

Category	Information Displayed
Interrupt	Interrupt number or name of an interrupt that might be generated.
CPU *number*	Number of interrupts that have occurred on a given processor.
Route-Trigger Method	How the interrupt is being delivered to the processor and the method of interrupting the processor.
Device	Name of the device driver that is generating the interrupt.

Figure 10-2 *Example Interrupt Information Page*

Interrupts

Interrupt Information			
Interrupt	**CPU0**	**Route-Trigger Method**	**Device**
0:	4,084,188	XT-PIC	timer
1:	1,132	XT-PIC	i8042
2:	0	XT-PIC	cascade
5:	0	XT-PIC	ehci_hcd
8:	2	XT-PIC	rtc
9:	93,026	XT-PIC	acpi, libata, eth0, uhci_hcd
10:	0	XT-PIC	uhci_hcd, Intel ICH5
11:	0	XT-PIC	uhci_hcd, uhci_hcd
12:	4,630	XT-PIC	i8042
14:	16,200	XT-PIC	ide0
15:	77	XT-PIC	ide1
NMI:	0		
LOC:	0		
ERR:	0		
MIS:	0		

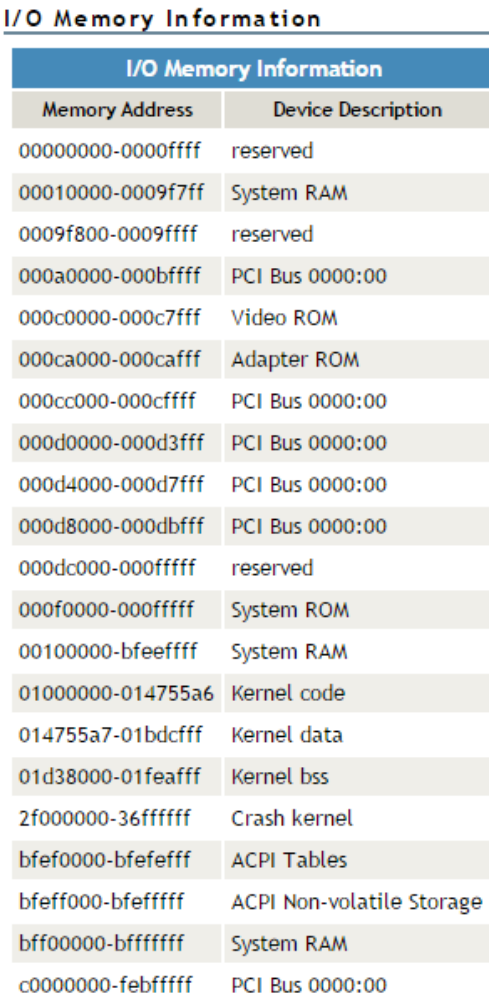
10.3 Viewing I/O Memory Information

Clicking the **IO Memory Information** link under the **Manage Hardware** heading in the navigation frame displays the I/O Memory Information page, which includes the following:

Table 10-3 *I/O Memory Information Page*

Category	Information Displayed
Memory Address	I/O memory range that a given device is using.
Device Description	A description of the device that is using a given I/O memory range.

Figure 10-3 *Example I/O Memory Information Page*



I/O Memory Information

I/O Memory Information	
Memory Address	Device Description
00000000-0000ffff	reserved
00010000-0009f7ff	System RAM
0009f800-0009ffff	reserved
000a0000-000bffff	PCI Bus 0000:00
000c0000-000c7fff	Video ROM
000ca000-000cafff	Adapter ROM
000cc000-000cffff	PCI Bus 0000:00
000d0000-000d3fff	PCI Bus 0000:00
000d4000-000d7fff	PCI Bus 0000:00
000d8000-000dbfff	PCI Bus 0000:00
000dc000-000fffff	reserved
000f0000-000fffff	System ROM
00100000-bfeeffff	System RAM
01000000-014755a6	Kernel code
014755a7-01bdcfff	Kernel data
01d38000-01feafff	Kernel bss
2f000000-36ffffff	Crash kernel
bfef0000-bfefefff	ACPI Tables
bfeff000-bfefffff	ACPI Non-volatile Storage
bff00000-bfffffff	System RAM
c0000000-febfffff	PCI Bus 0000:00

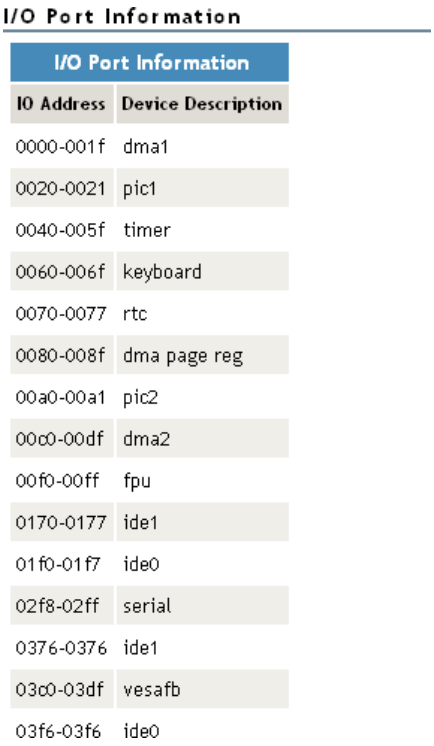
10.4 Viewing I/O Port Information

Clicking the **IO Port Information** link under the **Manage Hardware** heading in the navigation frame displays the I/O Port Information page, which includes the following:

Table 10-4 *IO Port Information Page*

Category	Information Displayed
IO Address	Shows the I/O port range that a given device is using.
Device Description	Shows the name of the device that is using a given I/O port range.

Figure 10-4 *Example I/O Port Information Page*



I/O Port Information

I/O Port Information	
IO Address	Device Description
0000-001f	dma1
0020-0021	pic1
0040-005f	timer
0060-006f	keyboard
0070-0077	rtc
0080-008f	dma page reg
00a0-00a1	pic2
00c0-00df	dma2
00f0-00ff	fpu
0170-0177	ide1
01f0-01f7	ide0
02f8-02ff	serial
0376-0376	ide1
03c0-03df	vesafb
03f6-03f6	ide0

10.5 Viewing SMBIOS Information

Clicking the **SMBIOS Information** link under the **Manage Hardware** heading in the navigation frame displays the SMBIOS Information page. On this page, you can view details about the BIOS hardware in each host without physically removing the hardware cover. You also have access to information that is available only through the management system.

Each link shows the type of device that is available in the BIOS of the host computer.

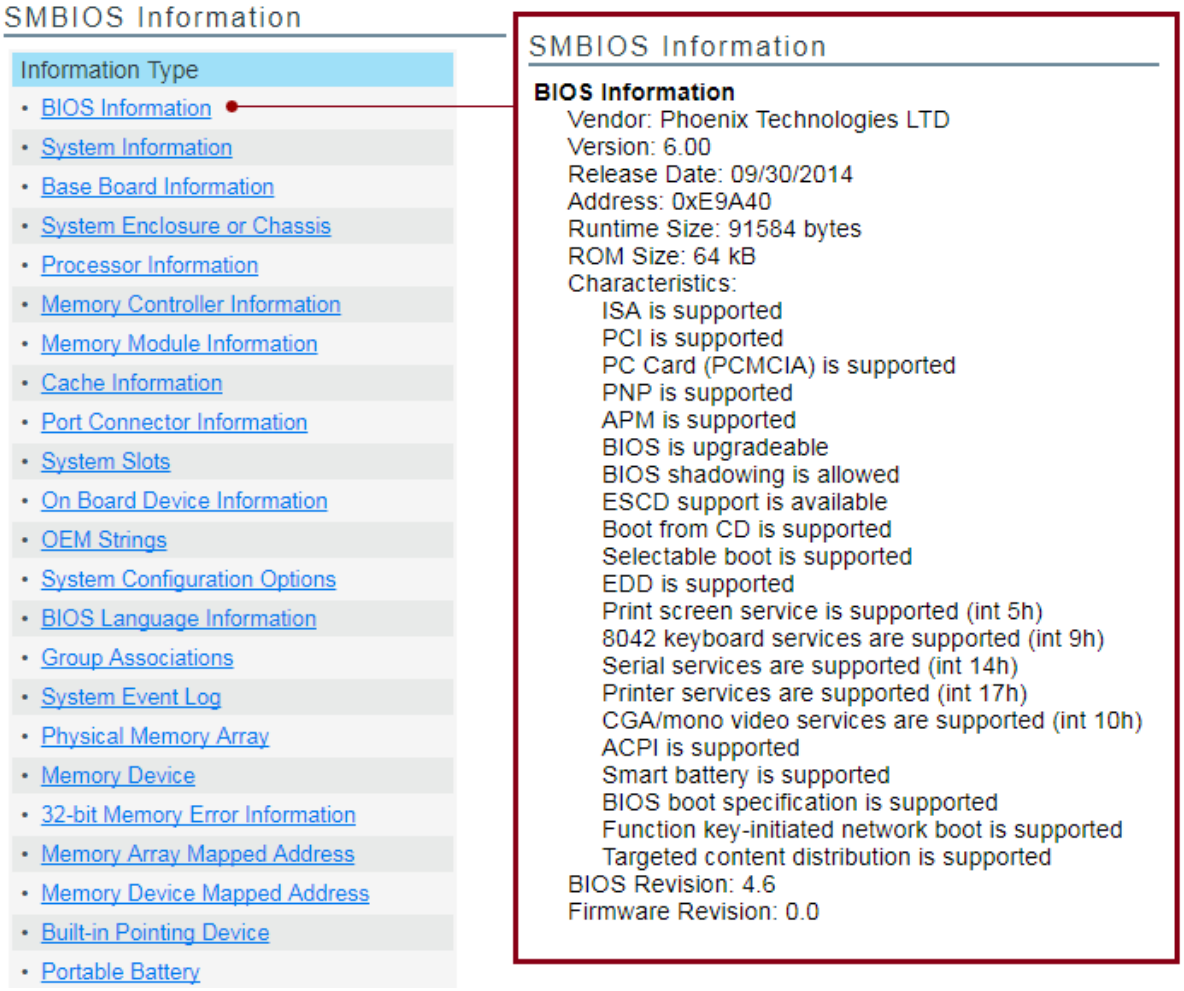
You might see information types such as the following. The types displayed vary depending on the hardware in your system.

- BIOS
- System
- Base Board
- System Enclosure or Chassis
- Processor
- Cache
- Port Connector
- System Slots
- On Board Device
- OEM Strings
- BIOS Language

- System Event Log
- Physical Memory Array
- Memory Device
- Memory Array Mapped Address
- Memory Device Mapped Address
- Hardware Security
- System Boot

Selecting an information type displays information contained within SMBIOS for the type selected. For example, to see all the BIOS information, click the **BIOS Information** link. See Figure 10-5.

Figure 10-5 *Example SMBIOS and BIOS Information Pages*



11 Using Group Operations

The **Use Group Operations** section in OES Remote Manager (NRM) for Linux includes the following links to pages from which you can perform the following tasks:

Table 11-1 *Use Group Operations Tasks, Links, and Pages*

Task	Link	Page Displayed	For More Information
Access an existing group	**Select Group**	Select Group	"Accessing an Existing Group" on page 95
Build and configure a new monitoring group	**Configure New Group**	Group Monitoring Operations	"Building and Configuring a Monitoring Group" on page 90
Change an existing group	**Select Group**	Select Group	"Changing an Existing Group" on page 95
Define or edit Group Monitoring types	**NRM Health Types**	OES Remote Manager Health Monitoring Engine (NRM Health Types)	"Defining or Editing Group Monitoring Types" on page 98
Delete an existing group	**Select Group**	Select Group	"Deleting an Existing Group" on page 96
Scan the network for items to monitor on the network.	**Configure New Group** > **right-click** > click **Network Discovery**	Network Discovery	"Discovering Items on the Network to Monitor" on page 99
Generate and view server reports	**Configure New Group** > **right-click** > click **Save Group**	Group Monitoring Operations	"Generating and Viewing Server Reports" on page 96
Save a new group	**Configure New Group** > **right-click** > click **Save Group**	Save Group	"Saving a Group" on page 94
View group operations monitored items	**View Monitored Items**	OES Remote Manager Health Monitoring Engine - Monitored Items	"Viewing Monitored Items" on page 97
View group operations defined NRM health types	**NRM Heath Types**	OES Remote Manager Health Monitoring Engine - NRM Health Types	"Viewing Group Monitoring Types" on page 98

NOTE

- For all group operations to function properly upgrade to OES 2018 SP3 or patch OES 2018 SP1 and OES 2018 SP2 with July patch.
- Group monitoring is supported for servers in the same eDirectory tree.

Using the group features involves performing one or more of the following tasks:

1. Building and Configuring a Monitoring Group (page 90).
2. (Optional) Saving a Group (page 94).

   You only need to perform this step if you want to use the group at a later time.
3. Generating and Viewing Server Reports (page 96).

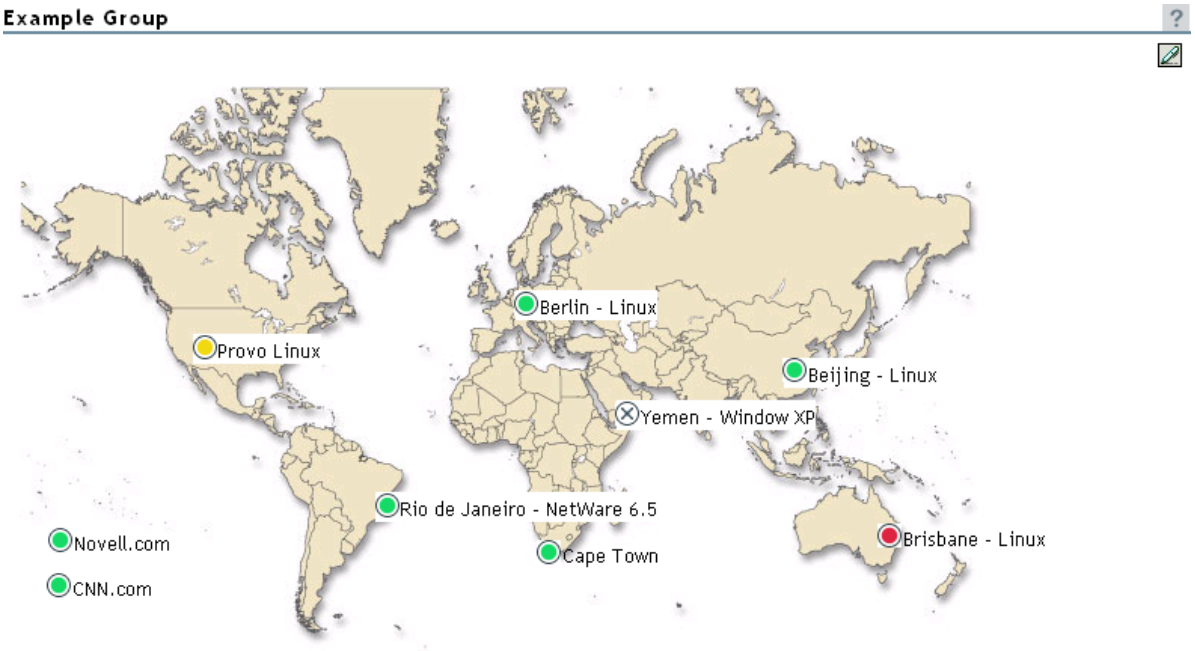
   The monitoring operations start immediately. Other tasks, such as running reports require additional steps.
4. (Conditional) Accessing an Existing Group (page 95).

11.1 Building and Configuring a Monitoring Group

OES Remote Manager lets you build and configure groups of items for monitoring Linux server health, as well as providing various statistics for servers running other operating systems. A few of the preconfigured monitoring item types are NRM Health Status for a single server or a group of servers, Ping to a specific port, IP connectivity, LDAP Directory Root Search, and status of connectivity to a web page.

Monitoring items can be defined and represented by an icons on a page as shown in the following figure. The icons can represent a single item or a group of items.

Figure 11-1 *NRM Server Health Example Group*



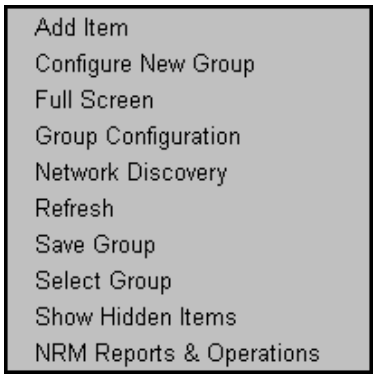
To build and configure a new monitor group:

1 Click the **Configure New Group** link in the navigation frame.

2 Right-click the Group Monitoring Operations page.

TIP: If your browser does not support right-click functionality, try double-clicking the Reports icon in the upper right corner of the page.

You should see a pop-up similar to the following:

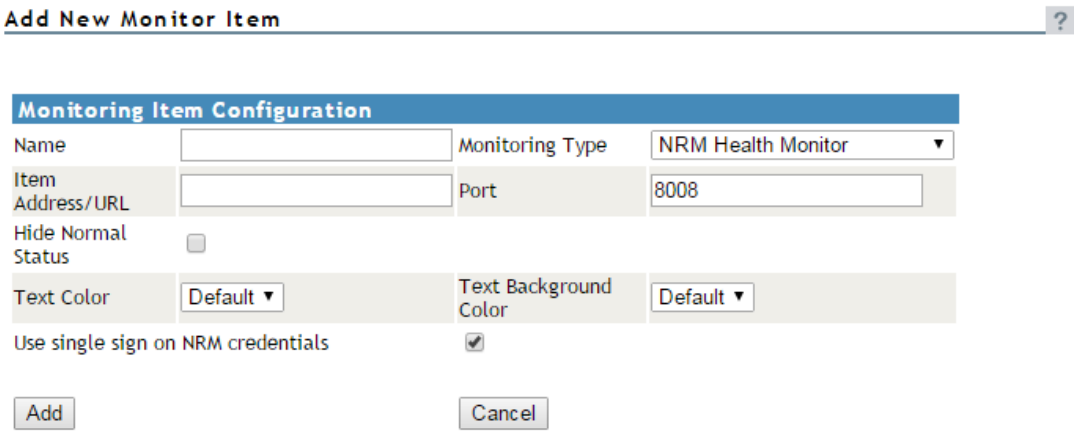


The menu options are:

- Add Item
- Configure New Group
- Full Screen
- Group Configuration
- Network Discovery
- Refresh
- Save Group
- Select Group
- Show Hidden Items
- NRM Reports & Operations

3 Click **Add Item**, and do the following:

3a Complete the Monitoring Item Configuration form.



For each item you add to a group or want to change from the default setting (health monitor), complete the following options on the Monitoring Item Configuration form.

Option	Details
Monitoring Type	Specify one of the following types: ◆ **Label:** Text information to use as a label on the group monitor display. Lets you identify each group specifically as needed. ◆ **LDAP Directory Root Search:** Shows the response when trying to ping port 389 of the specified LDAP server. Credentials are not used. This is useful to monitor the status of your LDAP servers in your network. ◆ **NRM Group:** Shows the health status of a group of servers. Lets you access the specific health page for each server in the group. ◆ **NRM Health Monitor:** Shows the health status of each server in the group. Lets you access the specific health page for each server in the group. ◆ **Ping (ICMP):** Shows the response when sending ping requests to the specified DNS name or IP address. ◆ **TCP/IP Port Query:** Shows response activity of a designated TCP/IP service. This query attempts to make a TCP connection to the specified address and port. Returns green (good) health if any services is listening. For example, you could set up a health monitoring item to tell you whether your GroupWise server is still listening for logins from clients. The only states that are returned are green (good), which means the connection was successful, and red (bad), which means the connection was not successful. ◆ **Web page:** Shows the response when trying to determine if the communication is working to a server that hosts a website. It does not monitor specific websites on the server. It does not monitor whether the web service is running. Specify only the portion of the web address (URL) that a DNS server can resolve to an IP address; do not include a subdirectory. For example, specify `www.novell.com`, but not `www.novell.com/support`. If you specify a subdirectory, the DNS name cannot be resolved, and a Can't Connect health status is reported.
Name	Provide a descriptive name for the item.
Item Address/URL	Specify the IP address for the server that you want to monitor or ping, or specify the DNS name of the server that hosts the web page. The address can be an IP address or DNS name. Do not specify the HTTP:// portion of a URL.
Port	The default is provided. You can type a different port to use.
Use Single Sign on NRM Credentials	When selected (default), the credentials used to access this items' data are the same as the credentials that the user logged into OES Remote Manager with. When deselected, enter the credential necessary to access the item in the User Name and Password fields.

Option	Details
Hide Normal Status	When selected, only items that are in an abnormal state are displayed. If you want to monitor all statuses, leave the check box deselected.
Text Color	Black is the default. You can select any other color from the drop-down list.
Text Background Color	Clear is the default. You can select any other color in the drop-down list.

You can also define your own monitoring types or edit the default defined health types by editing the XML data in `/opt/novell/nrm/NRMGroupHealthInfo` file. For more information, see "Defining or Editing Group Monitoring Types" on page 98.

3b Click **Add**.

3c Drag the monitor items to the desired location.

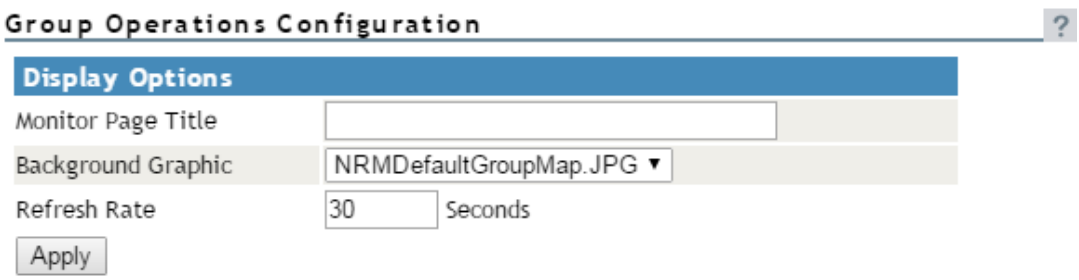
3d Repeat Step 3a through Step 3c for each item that you add.

4 (Optional) If you want to change any of the following, change the configuration of the group:

- The label for the group
- The graphic displayed
- The refresh rate
- The suspect and critical email notification for the group

4a Right-click the customized Group page, then click **Group Configuration**.

4b Complete the fields as desired on the Group Operations Configuration form.



Option	Description
Display	The display options let you control the following: • **Monitor Page Title:** Specify a title to be shown at the top of the monitor page in the header area when the page is built. • **Refresh Rate:** Specify the number of seconds between status queries to the server. • **Background Graphic:** Select a graphic from the drop-down list for the monitor items to be displayed on. This option can be helpful if you want to show specific locations of the item being monitored. If you want to add a customized graphic, add it to the `/opt/novell/nrm/NRMGroupMaps` directory.

4c Click **Apply**.

5 Perform the desired task, or save the group and perform the task later.

In this release, the only task you can perform on Linux servers is to compare the server up times.

6 (Optional) If you want to reuse the group, save the group.

6a Right-click the *customized Group page*, then click **Save Group**.

We recommend using a name that represents the group you built.

6b (Conditional) If you haven't saved any groups, you might need to extend the schema for NRM group operations before you can save the group.

Extending the schema is required only once per eDirectory tree. If the host is connected to a pre-existing NetWare 6.5 or later network, then extending the schema is not necessary.

6c Click **Save Group** and perform the required steps to save the group to a local server or save it and associate it with an eDirectory object.

See "Saving a Group" on page 94.

11.2 Saving a Group

You can save the configuration of the group so you can access this page again without completing the configuration options. You can save a group to the local server or associate with an eDirectory object and save it.

11.2.1 Saving the Group to the Local Server

1 While viewing the group you just created or edited, right-click the *customized Group* page, then click **Save Group**.

2 In the **Group Name** field, specify a name for the group or select a group name that you want to replace from the group list.

We recommend using a name that represents the group you built.

3 Click **Save Group**.

This saves the group to a file with that name in the `/opt/novell/nrm/NRMGroups` directory.

11.2.2 Saving the Group and Associating It with an eDirectory Object

You can save a group and associate it with a User or Group eDirectory object. This is helpful when you want to access the configuration and you don't want to save the configuration to a specific server (for example, if the server is down but you want it to be part of the operation or if you want to run the operation while one of the servers is not functioning properly).

Only one group can be associated to an object.

1. While viewing the group you just created or edited, right-click the *customized Group* page, then click **Save Group**.
2. In the **Make This the Group Monitor for This Object** field, specify a User or Group object that you want to associate this group with.

   You can browse to the user or group by clicking the **Browse** link icon or by typing the full content name of the object.
3. Click **Save Group**.

11.3 Accessing an Existing Group

After a group has been saved to the server, you can access the group again to run reports or change the attributes of the group.

1. Click the **Select Group** link in the navigation frame.
2. On the Server Group page, select the desired group from the drop-down list.
3. Click **Build Group**.

11.4 Changing an Existing Group

After accessing an existing group (see "Accessing an Existing Group" on page 95), you might want to change it using one of the following procedures.

Table 11-2 *Changing an Existing Group Tasks and Procedures*

If you want to	Then
Change the configuration of an existing group.	1. Select the group. 2. Right-click the page, then click **Group Configuration**. 3. Make the desired changes in the Group Operations Configuration form. 4. Click **Apply**. 5. Save the group. (See "Saving a Group" on page 94.)
See the details of the server health or the monitoring type.	1. Select the group. 2. Select the item you want to see the details for. 3. Double-click the **Health Status** icon.

If you want to	Then
Edit an existing item in the group.	1. Select the group. 2. Select the item you want to edit. 3. Right-click the selected item. 4. Click **Edit**.
Delete a server or monitor item from a group.	1. Select the group. 2. Select the item you want to delete. 3. Right-click the selected item. 4. Click **Delete**.
Change the display to a full screen in your browser window.	1. Select the group. 2. Right-click the page. 3. Click **Full Screen** 4. When you are finished viewing the group, close the browser window.

11.5 Deleting an Existing Group

To delete a group:

1. Click the **Select Group** link in the navigation frame.
2. On the Server Group page, select the desired group from the drop-down list.
3. Click **Delete Group**.

11.6 Generating and Viewing Server Reports

Running Server Comparison reports on a group of servers can help you in determine which servers need to be updated or have configurations changed, why operations on that server might be sluggish, or which servers are receiving the most action.

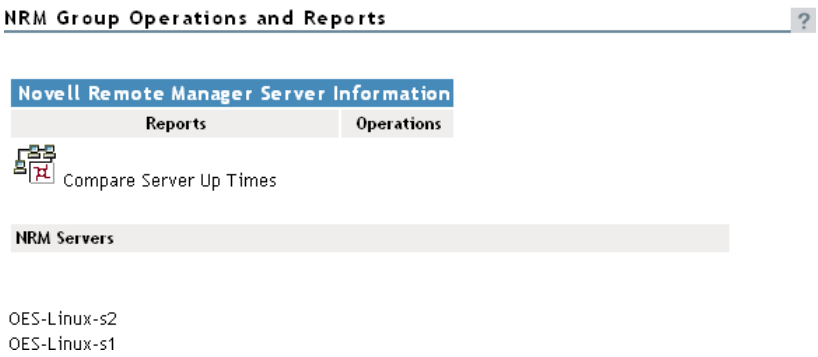
In this release, you can run only one report, the “Compare Server Up Time Report” on page 96.

11.6.1 Compare Server Up Time Report

Run this report to see which servers might need replacing or tuning to keep them running longer. This report gives you an idea how long each server in the group has been running without being restarted.

1. Build the monitor group or select a group previously saved.

   See “Building and Configuring a Monitoring Group” on page 90 or “Accessing an Existing Group” on page 95.
2. Right-click the customized Group page.
3. Click **NRM Reports & Operation**.



4 Click **Compare Server Up Times**.

A report similar to the following is returned.

Server Up Time Report
Server
Up Time
OES-Linux-s2 16 days 06 hours 05 minutes 46 seconds
OES-Linux-s1 14 days 22 hours 58 minutes 08 seconds
Server has been up less than one hour.
Server has been up less than one day.

11.7 Viewing Monitored Items

If you have several groups defined and you want to see which items are being monitored from this server without opening each group, click **View Monitored Items**.

This page lists of all of the items currently being monitored by the OES Remote Manager overall health monitoring engine on this server. For information about how this status is calculated for an OES server, see "Viewing the Overall Server Health Status" on page 40.

If an item has not been monitored for more than 3 minutes, it is removed from the list.

Table 11-3 *Health Monitoring Engine Monitored Items*

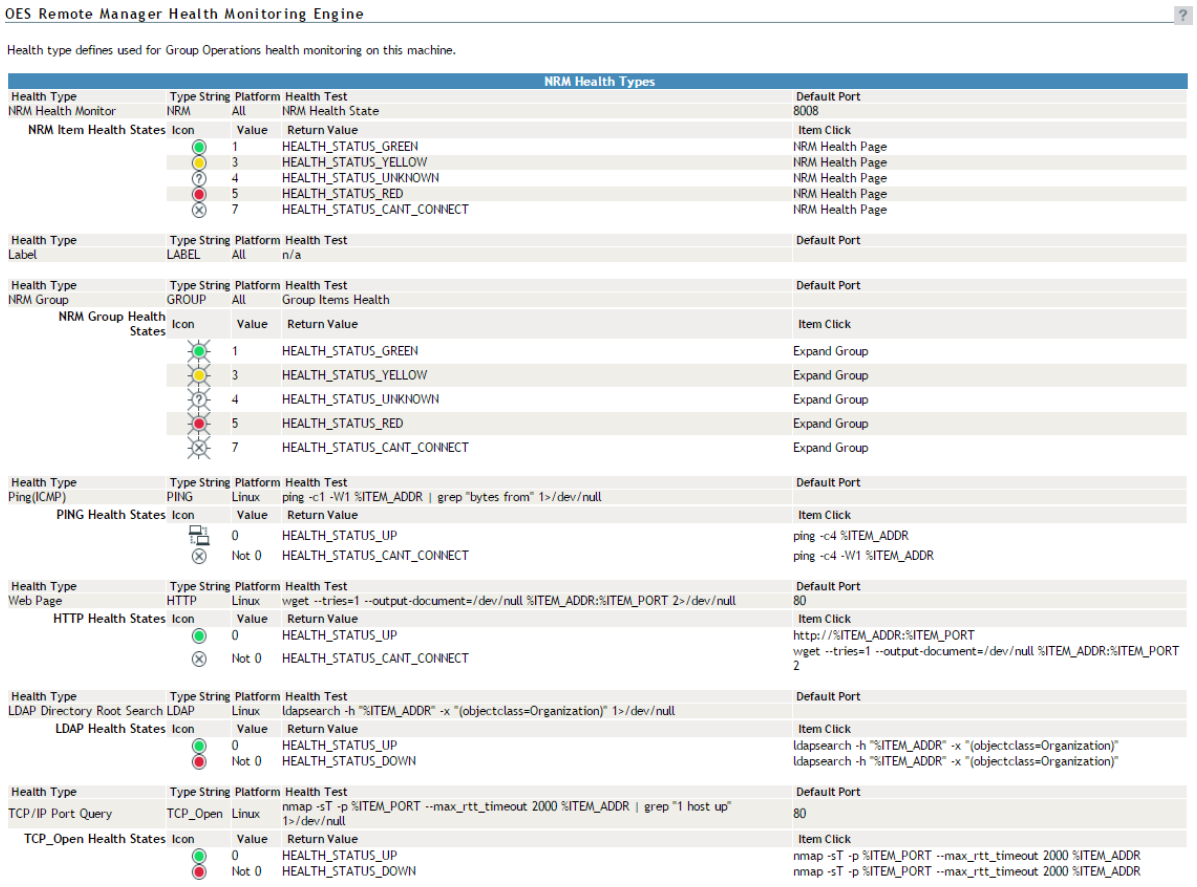
Column	Description
Status	Shows the overall health indicator icon for the item
Item Name	The name assigned to the item when it was defined in a OES Remote Manager health monitoring group.
Type	The type of item being monitored, such as NRM health, ping status, web page.
Address	The third column is the address that OES Remote Manager uses to check the items health status.
Last Check Time	The last time that a OES Remote Manager group requested the health status of this item.
Monitoring Start Time	The that health monitoring was started for this item.

If this server's utilization is high due to the monitoring occurring on this server, you might consider moving some of the monitoring to another location.

11.8 Viewing Group Monitoring Types

Clicking the **NRM Health Types** link in the navigation frame displays the OES Remote Manager Health Monitoring Engine - NRM Health Types content. This page gives you an overview of the Group Monitoring types that are defined on the current host. The legend shows the statuses you might see when you are monitoring groups of hosts with various monitored items and is a graphical view of the items defined in the `/opt/novell/nrm/NRMGroupHealthInfo` file.

Figure 11-2 *The Default NRM Health Monitoring Engine - NRM Health Types Content Definitions*



OES Remote Manager Health Monitoring Engine

Health type defines used for Group Operations health monitoring on this machine.

NRM Health Types

Health Type	Type String	Platform	Health Test	Default Port
NRM Health Monitor	NRM	All	NRM Health State	8008
NRM Item Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		1	HEALTH_STATUS_GREEN	NRM Health Page
		3	HEALTH_STATUS_YELLOW	NRM Health Page
		4	HEALTH_STATUS_UNKNOWN	NRM Health Page
		5	HEALTH_STATUS_RED	NRM Health Page
		7	HEALTH_STATUS_CANT_CONNECT	NRM Health Page
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
Label	LABEL	All	n/a	
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
NRM Group	GROUP	All	Group Items Health	
NRM Group Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		1	HEALTH_STATUS_GREEN	Expand Group
		3	HEALTH_STATUS_YELLOW	Expand Group
		4	HEALTH_STATUS_UNKNOWN	Expand Group
		5	HEALTH_STATUS_RED	Expand Group
		7	HEALTH_STATUS_CANT_CONNECT	Expand Group
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
Ping(ICMP)	PING	Linux	ping -c1 -W1 %ITEM_ADDR | grep "bytes from" 1>/dev/null	
PING Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		0	HEALTH_STATUS_UP	ping -c4 %ITEM_ADDR
		Not 0	HEALTH_STATUS_CANT_CONNECT	ping -c4 -W1 %ITEM_ADDR
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
Web Page	HTTP	Linux	wget --tries=1 --output-document=/dev/null %ITEM_ADDR:%ITEM_PORT 2>/dev/null	80
HTTP Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		0	HEALTH_STATUS_UP	http://%ITEM_ADDR:%ITEM_PORT
		Not 0	HEALTH_STATUS_CANT_CONNECT	wget --tries=1 --output-document=/dev/null %ITEM_ADDR:%ITEM_PORT 2
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
LDAP Directory Root Search	LDAP	Linux	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)" 1>/dev/null	
LDAP Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		0	HEALTH_STATUS_UP	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)"
		Not 0	HEALTH_STATUS_DOWN	ldapsearch -h "%ITEM_ADDR" -x "(objectclass=Organization)"
Health Type	**Type String**	**Platform**	**Health Test**	**Default Port**
TCP/IP Port Query	TCP_Open	Linux	nmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR | grep "1 host up" 1>/dev/null	80
TCP_Open Health States	**Icon**	**Value**	**Return Value**	**Item Click**
		0	HEALTH_STATUS_UP	nmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR
		Not 0	HEALTH_STATUS_DOWN	nmap -sT -p %ITEM_PORT --max_rtt_timeout 2000 %ITEM_ADDR

11.9 Defining or Editing Group Monitoring Types

If you want to add a Group Monitoring type to the group monitoring that is not defined or change the label of any of the predefined types, you can access the `/opt/novell/nrm/NRMGroupHealthInfo` file and make changes to it.

Each item is defined between the beginning and ending NRM_Health_Item_Definition XML tags as shown below.

```
<NRM_Health_Item_Definition>
   <Type_Name>PING</Type_Name>
   <Display_Name>Ping(ICMP)</Display_Name>
   <Platform>Linux</Platform>
   <Health_Test>
      <Command_Line>
         ping -c1 -W1 %ITEM_ADDR | grep "bytes from" 1>/dev/null
      </Command_Line>
      <Result>
         <Value>0</Value>
         <Result_Icon>/sys/login/NRMcanping.gif</Result_Icon>
         <Return_Value>HEALTH_STATUS_UP</Return_Value>
         <Click_Command>ping -c4 %ITEM_ADDR</Click_Command>
      </Result>
      <Result>
         <!Value>0</!Value>
         <Return_Value>HEALTH_STATUS_CANT_CONNECT</Return_Value>
         <Click_Command>ping -c4 -W1 %ITEM_ADDR</Click_Command>
      </Result>
   </Health_Test>
</NRM_Health_Item_Definition>
```

11.10 Discovering Items on the Network to Monitor

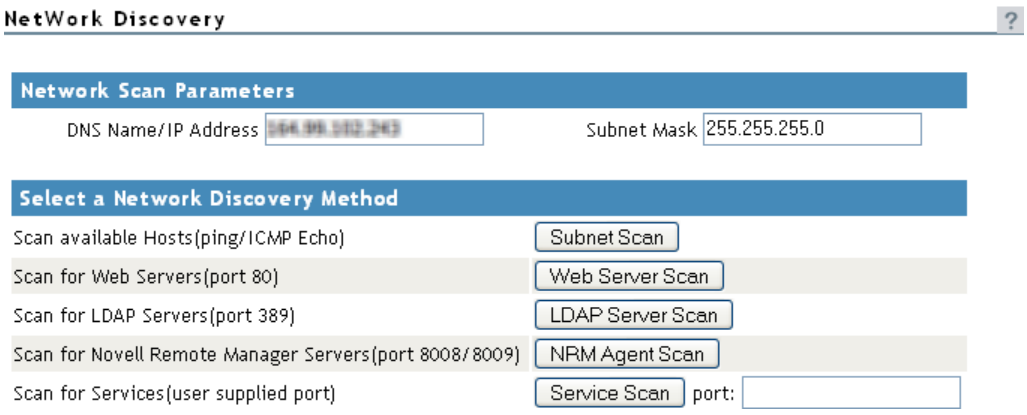
If you want to scan the network for specific services, you can access the Network Discovery page and specify the host and ports that should be scanned for. After discovering the items on the network, you can click the item and add it to the current group for future monitoring.

Using this feature can help you to quickly gather the information you need to create monitoring groups.

To access this page, do the following:

1. In the navigation frame, click **Use Group Operations** > **Configure New Group** or **Select Group**.
2. Right-click the applicable group page displayed.
3. Verify that the browser you are using will accept pop-up dialog boxes.
4. Click **Network Discovery**.

   The Network Discovery page is displayed:



To perform the scan, do the following:

1. Access the Network Discovery page.
2. Do the tasks specified in the following table:

   The **Network Scan Parameter** fields determine which hosts or ports should be scanned.

   The **DNS Name / IP Address** field is an IP address is used with the subnet mask to determine the range of IP addresses to be scanned. These fields default to the IP address of the current OES Remote Manager host and a class C subnet mask. For example, if you wanted to scan for all the active hosts in the class B range of 137.65 subnet, you might set the IP address to 137.65.1.1 and the subnet mask to 255.255.0.0.

   Instead of scanning for all hosts that respond on the network, you can scan for hosts with specific services available.

Task	Procedure
Scan the network for hosts that are responding to ICMP Echo Requests in the network within a specified subnet.	1. Accept the default IP address or DNS name and subnet mask information or change it. 2. Click **Subnet Scan**.
Scan the network for hosts with port 80 open and listening for connections (Web Servers) within a specified subnet.	1. Accept the default IP address or DNS name and subnet mask information or change it. 2. Click **Web Server Scan**.
Scan the network for hosts with port 389 open and listening for connections (LDAP Servers) within a specified subnet.	1. Accept the default IP address or DNS name and subnet mask information or change it. 2. Click **LDAP Server Scan**.
Scan the network for hosts with port 8009 open and listening for connections (Hosts with OES Remote Manager configured for the default ports) within a specified subnet.	1. Accept the default IP address or DNS name and subnet mask information or change it. 2. Click **NRM Agent Scan**.
Scan the network for hosts with *user_defined_port* open and listening within a specified subnet.	1. Accept the default IP address or DNS name and subnet mask information or change it. 2. Click **Service Scan**.

   After scanning for a desired service, a Network Discovery page is displayed showing results for all hosts with the ports.

You can do the following task with the information returned:

Task	Procedure
See more information about the scanned host.	1. Click the **Web Service More Info** icon for the applicable host on the Network Discovery page. 2. View the information on the page that is returned.
Add the host to the current group.	1. Click the **Add Item to Group** icon for the applicable host on the Network Discovery page. 2. Complete the required information on the Add New Monitor Item page, then click **Add**. Most of the information is completed by default.

12 Managing NCP Services

This section provides an overview of tasks that can be performed when the **NCP Server and Dynamic Storage Technology** plug-in is installed in OES Remote Manager.

For information about using and managing NCP Server and NCP volumes on Open Enterprise Server (OES), see the *OES 2018 SP3: NCP Server for Linux Administration Guide*.

For information about using and managing NSS volumes on OES, see the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

The **Manage NCP Services** section in OES Remote Manager for Linux includes the following links to these pages:

Table 12-1 *Links for Managing NCP Services*

Link	Page Displayed	For More Information
View Inventory Reports	NCP Inventory Reports ◆ Generate report ◆ Display last report	Section 12.3, "Generating Inventories for Directories or NCP Volumes," on page 119
View Trustee Reports	NCP Trustee Reports ◆ Generate report ◆ Display last report	Section 12.6, "Generating and Viewing NCP Trustee Reports for NSS Volumes," on page 128
Manage Shares	NCP Shares ◆ Active shares listing for NSS volumes and NCP volumes ◆ Information about shares, including open files ◆ Create new share ◆ Delete existing share ◆ NCP/NSS bindings	"Managing NCP Volumes" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*
Manage Server	NCP Manage Server ◆ Server parameters for NCP Server ◆ Global policy parameters for Dynamic Storage Technology	"Managing NCP Server" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*

Link	Page Displayed	For More Information
Manage Connections	Connections ◆ Connection information (statistics) ◆ Broadcast message to everyone ◆ Connection listing ◆ Detailed information about a connection, including open files	"Managing Connections for NCP Volumes and NSS Volumes" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*
View Logs	NCP System Logs ◆ Logs ◆ `ncpserv.log` ◆ `ncp2nss.log` ◆ Audit logs ◆ `ncpserv.audit.log` ◆ `ncp2nss.audit.log` ◆ `SYS.audit.log` `<volume_name>.audit.log`	"Log Files" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*
View Statistics	NCP Statistical Information ◆ Server information ◆ Server statistics	"NCP Server Statistics" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*
View Diagnostic Information	NCP Diagnostic Information ◆ NCP engine ◆ NSS interface daemon	Chapter 7, "Diagnosing Problems Using Ganglia and Nagios," on page 39

From these pages you can perform the following tasks:

- Section 12.1, "Quick Reference for the NCP Server Plug-In for OES Remote Manager for Linux," on page 105
- Section 12.2, "Browsing NSS Volumes and Performing Actions on Them," on page 110
- Section 12.3, "Generating Inventories for Directories or NCP Volumes," on page 119
- Section 12.4, "Generating a Custom Inventory Report from a File Inventory Report," on page 125
- Section 12.5, "Performing Actions on Files from Custom Reports," on page 126
- Section 12.6, "Generating and Viewing NCP Trustee Reports for NSS Volumes," on page 128

12.1 Quick Reference for the NCP Server Plug-In for OES Remote Manager for Linux

- Section 12.1.1, “NCP Volumes (NCP Shares),” on page 105
- Section 12.1.2, “NCP Server Parameters,” on page 106
- Section 12.1.3, “NCP Server Connections,” on page 106
- Section 12.1.4, “NCP Trustee Reports,” on page 107
- Section 12.1.5, “NCP Logs and Audit Logs,” on page 107
- Section 12.1.6, “NCP Server Statistics,” on page 108
- Section 12.1.7, “NCP Server Diagnostics,” on page 108
- Section 12.1.8, “Dynamic Storage Technology,” on page 109

12.1.1 NCP Volumes (NCP Shares)

Table 12-2 describes the management tasks available for the **Manage NCP Services > Manage Shares** task in OES Remote Manager for Linux.

Table 12-2 *Manage NCP Services > Manage Shares*

Subtasks	Management Tasks
Share Name link	Browse files and directories. View and set file system attributes for files and directories on NSS volumes. View file information. View directory information.
Mount/Unmount	Mount NCP volumes and NSS volumes to make them available to NCP clients. Unmount NCP volumes and NSS volumes to make them unavailable to NCP clients.
Info icon	NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics. Open files listed for each NCP connection. Add a shadow volume for the NCP volume. For unmounted DST shadow volumes, click the **Info** icon to remove the shadow volume relationship. Removing a shadow volume removes the entry in the `ncpserv.conf` file, but does not delete the volumes that make up the shadow volume.

Subtasks	Management Tasks
Create new share	Creates an NCP volume name (share) on a Linux POSIX file system (Ext3, XFS, or Reiser), and associates it to a path on your server. You are prompted for a volume (share) name and a path to the volume. This creates a mount point to the volume you specify and makes it accessible to NCP clients. **IMPORTANT:** You cannot use this method to create an NSS volume. You must use NSS tools to create and manage NSS volumes on Linux.
Delete existing share	Removes the NCP volume and path association for NCP volumes on Linux POSIX file systems (Ext3, XFS, or Reiser). This does not remove or delete data from the directory; it removes only the volume mount point that was created for the NCP share.
NCP/NSS bindings	View or modify whether NSS volumes are NCP accessible. If they are not accessible, the EXCLUDE_VOLUME *volumename* command is added to the `/etc/opt/novell/ncp2nss.conf` file. Use this option for NSS volumes on clusters where the load script handles NCP mount of NSS volumes. Use this option for NSS volumes that you want to use as the secondary storage area in a Dynamic Storage Technology shadow volume.

12.1.2 NCP Server Parameters

Table 12-3 describes the management task available for the **Manage NCP Services > Manager Server** task in OES Remote Manager for Linux.

Table 12-3 *Manage NCP Services > Manage Server*

Subtasks	Management Tasks
Server Parameter Information	View NCP Server parameters for the SET command and their current values. Click the **Parameter Value** link to modify the value. For a list of parameters and their default values, see "Configuring Global NCP Server Parameters"in the *OES 2018 SP3: NCP Server for Linux Administration Guide*.

12.1.3 NCP Server Connections

Table 12-4 describes the management tasks available for the **Manage NCP Services > Manage Connections** task in OES Remote Manager for Linux.

Table 12-4 *Manage NCP Services > Manage Connections*

Subtasks	Management Tasks
Connection information	View connection statistics. Clear all **Not Logged In** connections.
Connection listing	View a list of connections. Click the name link for the connection to view statistics for the connection and a list of its open files. Clear selected connections.
Name link for the connection	View statistics for the connection. View the network address, status, privileges, and security equivalence for a logged-in-user. Send a message to the selected connection.
Broadcast messages to everyone	Broadcast messages to all logged-in NCP users. The `DISABLE_BROADCAST` parameter must be disabled (value of 0) in order for broadcast messages to be sent. Users must be using a Novell Client version that supports receiving broadcast messages, and the client must be configured to receive messages.

12.1.4 NCP Trustee Reports

Table 12-5 describes the management tasks available for the **Manage NCP Services > View Trustee Reports** task in OES Remote Manager for Linux.

Table 12-5 *Manage NCP Services > View Trustee Reports*

Subtasks	Management Tasks
Generating an NCP Trustee report for NSS volumes	View the NCP Trustee Report. A volume's trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.
Viewing a saved NCP Trustee report	View the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.
Emailing a saved NCP Trustee report	For OES 11 SP1 and earlier, email an NCP volume's trustee report to addresses that are configured in the `httpstkd.conf` file.

12.1.5 NCP Logs and Audit Logs

Table 12-6 describes the management tasks available for the **Manage NCP Services > View Logs** task in OES Remote Manager for Linux.

Table 12-6 *Manage NCP Services > View Logs*

Subtasks	Management Tasks
Logs	Download and view the `ncpserv.log` and `ncp2nss.log`.
Audit logs	Download and view the following audit logs: ◆ `ncpserv.audit.log` All the operations performed by NCP Engine are logged into this file in XML format. For example, add trustee, remove trustee, volume mount and dismount, NSS event handler startup/shutdown, add/remove volume, create shadow volume, security sync, and kill NCP connections. No file operations are logged in this file. ◆ `ncp2nss.audit.log` The following ncp2nss events are logged into this file: Open command file, write command file, ncp2nss daemon halted, ncp2nss daemon running, NSS not detected, domain socket not created, domain socket not accessible, uneb not started, failed to import uneb symbols, failed to create uneb processing thread, ndp library not started, failed to import ndp library symbols, and failed to initialize ndp library. ◆ `SYS.audit.log` ◆ *`volumename`*`.audit.log` (an audit log is listed for each NSS volume)

12.1.6 NCP Server Statistics

Table 12-7 describes the management tasks available for the **Manage NCP Services > View Statistics** task in OES Remote Manager for Linux.

Table 12-7 *Manage NCP Services > View Statistics*

Subtasks	Management Tasks
Server information	View server name, server version, and product version. View the number of connections.
Server statistics	View server statistics such as up time, traffic, and caching memory use.

12.1.7 NCP Server Diagnostics

Table 12-8 describes the management tasks available for the **Manage NCP Services > Diagnostic Information** task in OES Remote Manager for Linux.

Table 12-8 *Manage NCP Services > Diagnostic Information*

Subtasks	Management Tasks
NCP engine	View statistics for NCP events. Click the **Process ID** (**PID**) link to view information about the currently running process.
NSS interface daemon	View statistics for NSS events. Click the **Process ID** (**PID**) link to view information about the currently running process.

12.1.8 Dynamic Storage Technology

Table 12-9 describes the management tasks available for the **View File Systems > Dynamic Storage Technology Options** task in OES Remote Manager for Linux.

Table 12-9 *View File Systems > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume information	View a list of NCP volumes and NSS volumes on the server. Click the **Add Shadow** link next to an NSS volume to view share information, where you can create a shadow volume. (NCP volumes are not supported as shadow volumes.) Click the **Inventory** link next to a shadow volume to view an inventory report for both the primary and secondary volumes. Click the **View Log** link next to an NSS volume to download a copy of the audit log for the selected volume.
Add Shadow link	This option takes you to the Share Information page. Scroll down to the **Volume Tasks** area to find the **Add Shadow Volume** task. The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations. **WARNING:** NSS volumes must already exist when you create the shadow volume. The **Create if not present** option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.
Inventory link	View statistics and graphical trend displays for the volume's files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).

Subtasks	Management Tasks
Volume information (**Info** icon)	NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics. Open files listed for each NCP connection. Add a shadow volume for the NCP volume. For unmounted DST shadow volumes, click the Info icon to access the dialog to remove the shadow volume relationship. This removes the entry in the `ncpserv.conf` file, but does not delete the volume itself. To unmount a shadow volume, click **Manage NCP Services > Manage Shares**, then click **Unmount** option next to the shadow volume.
Dynamic Storage Technology policies	Create a new policy. View a list of existing policies. Click the **Policy Name** link to modify or delete the policy.
Duplicate file resolution options	Set a global policy for how to handle duplicate files.
ShadowFS configuration	Set a global policy for whether to automatically start FUSE and Shadow File System at boot time.

12.2 Browsing NSS Volumes and Performing Actions on Them

The NCP Server plug-in to OES Remote Manager appears as “Manage NCP Services” in the left panel. NCP volumes and NSS volumes are listed as NCP Shares.

For detailed information about creating and managing NCP volumes, see the *OES 2018 SP3: NCP Server for Linux Administration Guide*.

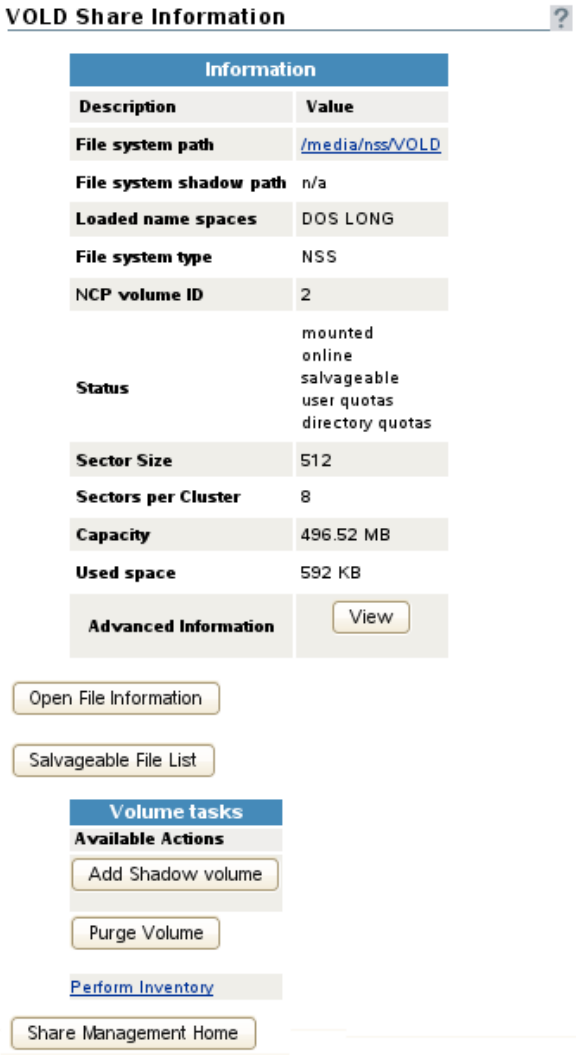
For detailed information about creating and managing NSS volumes, see the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

For detailed information about creating and managing Dynamic Storage Technology shadow volume pairs with NSS volumes, see the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

- Section 12.2.1, “Viewing Information about an NSS Volume,” on page 111
- Section 12.2.2, “Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It,” on page 113
- Section 12.2.3, “Viewing the Linux POSIX Details of a File and Performing Specific Actions on It,” on page 113
- Section 12.2.4, “Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files,” on page 114
- Section 12.2.5, “Salvaging and Purging Deleted Files on an NSS Volume,” on page 118
- Section 12.2.6, “Purging a Deleted NSS Volume,” on page 118
- Section 12.2.7, “Viewing Open File Information for an NSS Volume,” on page 119

12.2.1 Viewing Information about an NSS Volume

1. In OES Remote Manager, select **Manage NCP Services > Manage Shares**.
2. In the right pane, view the list of mounted NSS volumes in the **Active Shares** list.
3. Next to the volume name, click the **Information** icon (ⓘ) to go to the volume's Share Information page.



4. In the **Information** table, view the following information about the NSS volume:
   - File system path on Linux, such as `/media/nss/VOLD`

     Click the link to browse the directories and files on the volume.
   - File system shadow path, such as `/media/nss/SH_VOLD` (A path is displayed only when the specified NSS volume is the primary volume of a Dynamic Storage Technology shadow volume pair.)

     Click the link to browse the directories and files on the pair's secondary volume.
   - Loaded name spaces, such as DOS, LONG, MAC, and UNIX
   - File system type (NSS)

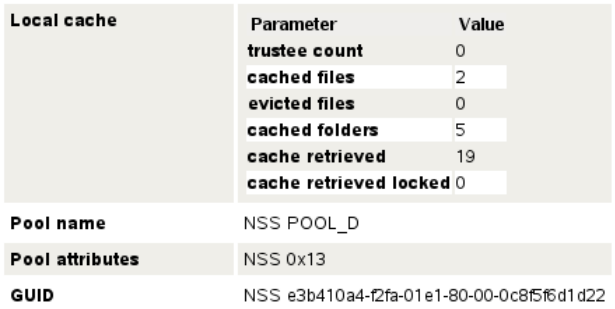
- NCP volume ID

  The NCP volume ID is a value between 0 and 254 that is automatically assigned for standalone volumes, beginning with zero. The SYS volume is by default assigned 0, and `_Admin` is assigned 1. For shared volumes, the volume ID is specified in the cluster load script for shared volumes, beginning with 254 and down.

- Status

  Identifies whether the volume is mounted/unmounted, online/offline, or in a cluster resource. It lists the NSS volume attributes that are enabled for the volume, such as Salvageable, User Quotas, Directory Quotas, and so on.

- Sector size
- Sectors per cluster
- Capacity
- Used space
- Advanced information (Click **View** to view.)



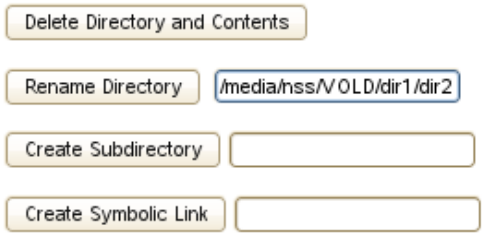
Local cache	Parameter	Value
	trustee count	0
	cached files	2
	evicted files	0
	cached folders	5
	cache retrieved	19
	cache retrieved locked	0
Pool name	NSS POOL_D	
Pool attributes	NSS 0x13	
GUID	NSS e3b410a4-f2fa-01e1-80-00-0c8f5f6d1d22	

  - Local cache
    - Trustee count
    - Cached files
    - Evicted files
    - Cached folders
    - Cache retrieved
    - Cache retrieved locked
  - Pool name
  - Pool attributes
  - GUID
- Open File Information (Click to view.)
- Salvageable Files (Click to view.)

12.2.2 Viewing the Linux POSIX Details of an NSS Directory and Performing Specific Actions on It

1. Click the **View File System Listing** link in the navigation frame, or click a **Mount Location** name link on the Home page.
2. On the Directory list page, browse to the `/media/nss/<volume_name>` directory and through its subdirectories to the directory, then click the **Directory Information** icon to the left of the directory name.
3. On the Directory Information page that is displayed, view the information about the file:
   - Directory owner
   - Group
   - Data modified time
   - Last accessed time
   - Information change time
   - Linux POSIX read/write/execute directory attributes.

   IMPORTANT: Do not use these settings for NCP and NSS volumes. Use the NCP view of the volume to set the OES Trustee Model attributes.
4. Perform any of the following tasks:



   - **Delete Directory and Its Contents:** Click this option to delete the selected directory and the subdirectories and files in it.
   - **Rename Directory:** Specify the full Linux path to the directory, including the new directory name, then click **Rename** Directory.
   - **Create Subdirectory:** Specify the name of the new subdirectory, then click **Create Subdirectory**.
   - **Create Symbolic Link:** Specify the name for the symbolic link, then click **Create Symbolic Link**.

12.2.3 Viewing the Linux POSIX Details of a File and Performing Specific Actions on It

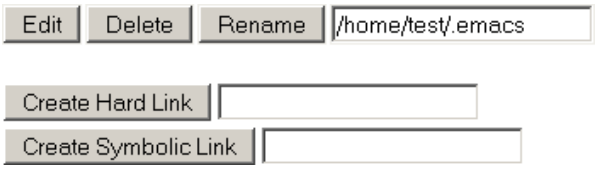
1. Click the **View File System Listing** link in the navigation frame, or click a **Mount Location** name link on the Home page.
2. On the Directory list page, browse to the `/media/nss/<volume_name>` directory and through its subdirectories to the file, then click the **File Info** icon to the left of the file name.

3 On the File Information page that is displayed, view the information about the file:

- File owner
- Group
- Data modified time
- Last accessed time
- Information change time
- Linux POSIX read/write/execute file attributes.

IMPORTANT: Do not use these settings for NCP and NSS volumes. Use the NCP view of the volume to set the Novell Trustee Model attributes.

4 Perform any of the following tasks:



- **Edit:** The **Edit** button is available only on simple text files or on files with the extensions listed in the `/opt/novell/nrm/nrmedit.txt` file. If you want to save the file with an ANSI or UTF-8 encoding, select the appropriate option and click **OK**.
- **Delete:** Click **Delete** to delete the selected file.
- **Rename:** Specify the full Linux path to the file, including the new file name, then click **Rename**.
- **Create Hard Link:** Specify the hard link path, then click **Create Hard Link**.
- **Create Symbolic Link:** Specify the symbolic link path, then click **Create Symbolic Link**.

12.2.4 Browsing an NSS Volume and Setting Rights and File System Attributes on Directories and Files

1 In OES Remote Manager, select **Manage NCP Services > Manage Shares**.

2 In the right pane, view the list of mounted NSS volumes in the **Active Shares** list.

3 Click the volume **Name** link to view a folder list and to browse the files on the NSS file system.

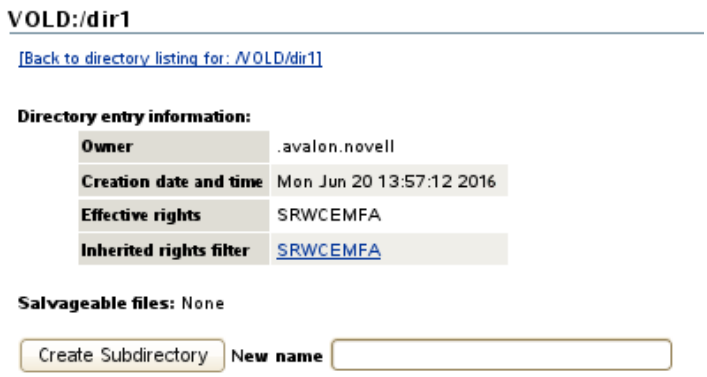
Click the arrows in the column headings to sort the list by name, type (file extension), size, or last modified date and time.

4 Use the links above the file list to perform the following actions on the volume:

- **Upload**
- **Text Search**
- **File Search**
- **Inventory**

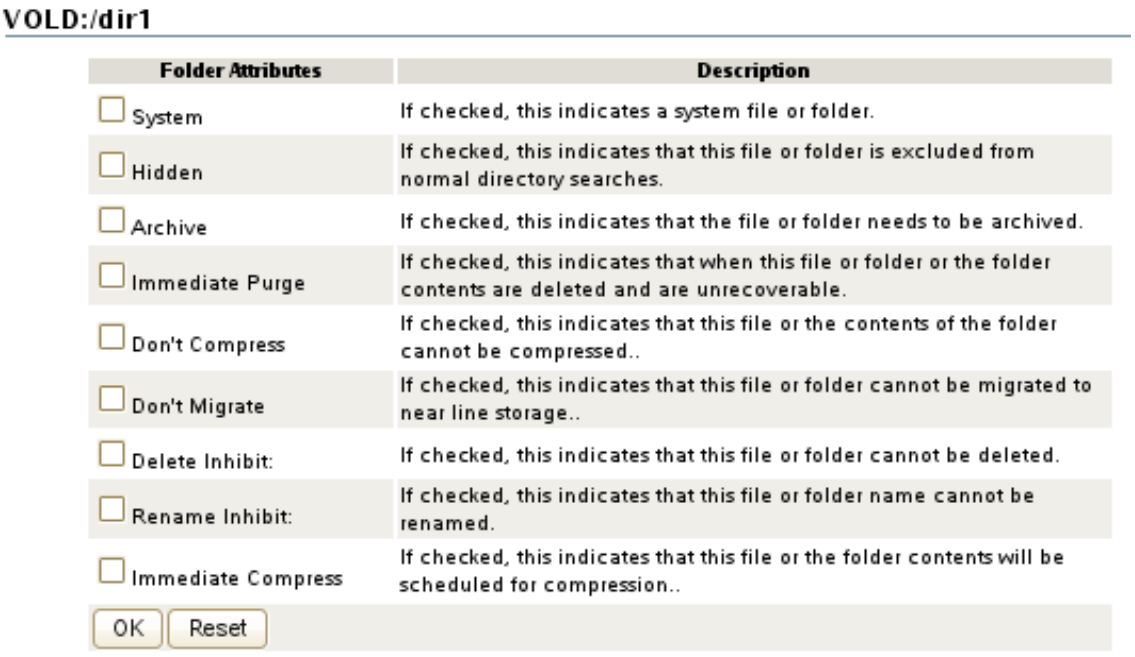
For information, see Section 12.3, “Generating Inventories for Directories or NCP Volumes,” on page 119.

5 Click a directory's **Directory Information** icon to view information about the directory. You can also create subdirectories.



- Owner
- Creation date and time
- Effective rights (based on the OES Trustee Model)
- Inherited rights filter (based on the OES Trustee Model). You can click the link to modify the rights inheritance filter settings.
- Salvageable files

6 Click a directory's **Attributes** link to view or modify the NSS file system attributes that are set for the directory. Click **OK** to save your changes.


VOLD:/dir1
Folder Attributes
Description
System
If checked, this indicates a system file or folder.
Hidden
If checked, this indicates that this file or folder is excluded from normal directory searches.
Archive
If checked, this indicates that the file or folder needs to be archived.
Immediate Purge
If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.
Don't Compress
If checked, this indicates that this file or the contents of the folder cannot be compressed..
Don't Migrate
If checked, this indicates that this file or folder cannot be migrated to near line storage..
Delete Inhibit:
If checked, this indicates that this file or folder cannot be deleted.
Rename Inhibit:
If checked, this indicates that this file or folder name cannot be renamed.
Immediate Compress
If checked, this indicates that this file or the folder contents will be scheduled for compression..
OK
Reset

- System
- Hidden
- Archive
- Immediate purge

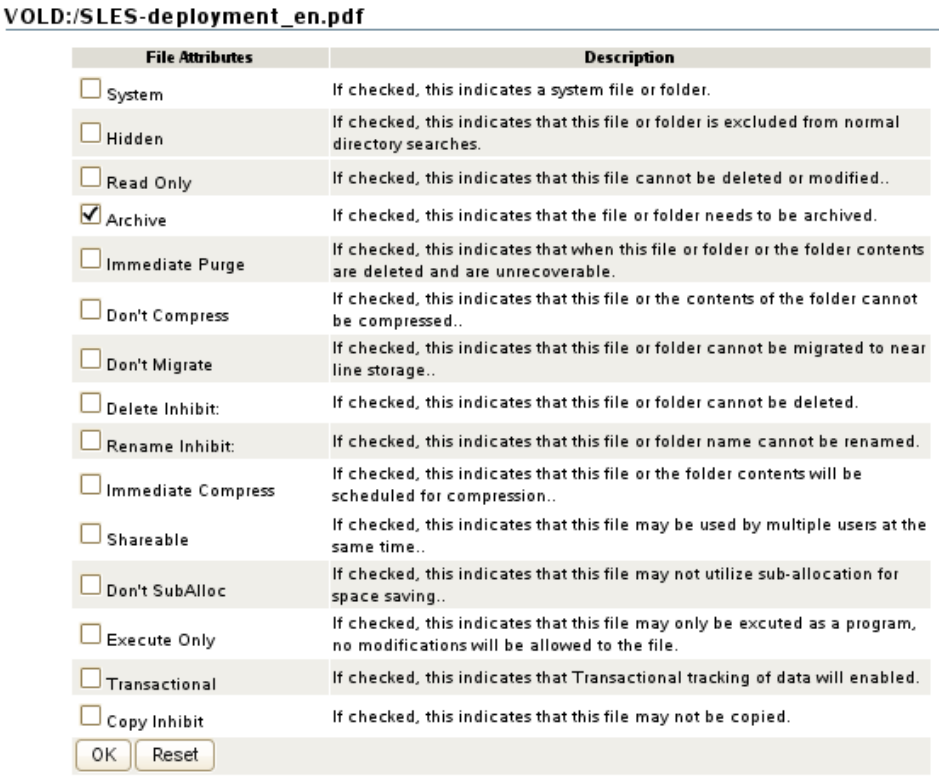
- Do not compress
- Do not migrate
- Delete inhibit
- Rename inhibit
- Immediate compress

For information about the meaning and usage of NSS file system attributes for directories, see "Understanding Directory and File Attributes for NSS Volumes" in the *OES 2018: File Systems Management Guide*.

7 Click a file's **File Information** icon to view the following file information. You can also delete the file from this page by clicking **Delete File**.

- Owner
- Last modified date and time
- Creation date and time
- Last archived date and time
- Effective rights (based on the OES Trustee Model)
- Inherited rights filter (based on the OES Trustee Model). You can click the link to modify the rights inheritance filter settings.
- Disk space in use

8 Click a file's **Attributes** link to view or modify the NSS file system attributes that are set for the file. Click **OK** to save your changes.



VOLD:/SLES-deployment_en.pdf

File Attributes	Description
☐ System	If checked, this indicates a system file or folder.
☐ Hidden	If checked, this indicates that this file or folder is excluded from normal directory searches.
☐ Read Only	If checked, this indicates that this file cannot be deleted or modified..
☑ Archive	If checked, this indicates that the file or folder needs to be archived.
☐ Immediate Purge	If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.
☐ Don't Compress	If checked, this indicates that this file or the contents of the folder cannot be compressed..
☐ Don't Migrate	If checked, this indicates that this file or folder cannot be migrated to near line storage..
☐ Delete Inhibit:	If checked, this indicates that this file or folder cannot be deleted.
☐ Rename Inhibit:	If checked, this indicates that this file or folder name cannot be renamed.
☐ Immediate Compress	If checked, this indicates that this file or the folder contents will be scheduled for compression..
☐ Shareable	If checked, this indicates that this file may be used by multiple users at the same time..
☐ Don't SubAlloc	If checked, this indicates that this file may not utilize sub-allocation for space saving..
☐ Execute Only	If checked, this indicates that this file may only be excuted as a program, no modifications will be allowed to the file.
☐ Transactional	If checked, this indicates that Transactional tracking of data will enabled.
☐ Copy Inhibit	If checked, this indicates that this file may not be copied.
OK Reset	

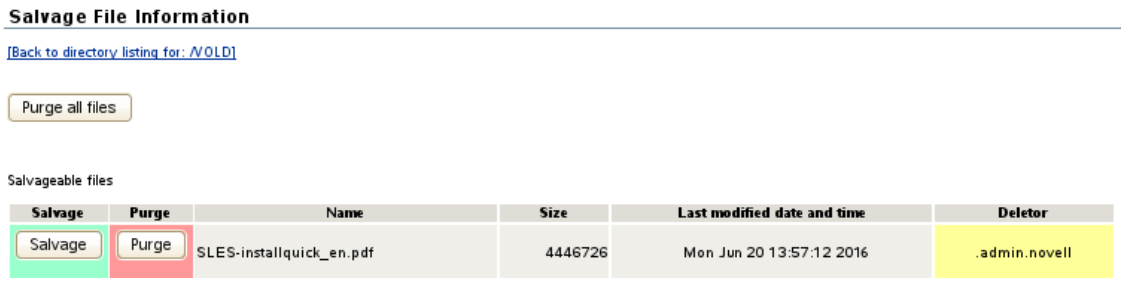
- System
- Hidden
- Read only
- Archive
- Immediate purge
- Do not compress
- Do not migrate
- Delete inhibit
- Rename inhibit
- Immediate compress
- Shareable
- Do not suballocate
- Execute only
- Transactional
- Copy inhibit

For information about the meaning and usage of NSS file system attributes for directories, see "Understanding Directory and File Attributes for NSS Volumes" in the *OES 2018: File Systems Management Guide*.

12.2.5 Salvaging and Purging Deleted Files on an NSS Volume

From an NSS volume's Share Information page, the **Salvageable File List** option allows you to view a list of deleted files that are available for salvage or purge on the volume. Deleted files are available only for NSS volumes where the Salvage attribute is enabled. For information about the NSS file salvage feature, see "Volume Salvage versus File Salvage" in the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

1. In OES Remote Manager, select **Manage NCP Services > Manage Shares**.
2. In the right pane, view the list of mounted NSS volumes in the **Active Shares** list.
3. Next to the volume name, click the **Information** icon (I) to go to the volume's Share Information page.
4. Below the **Information** table, click **Salvageable File List** to open the Salvage File Information page.



5. Salvage or purge files in the list:

   If the deleted file resided in a directory that has been deleted, you must first salvage the deleted directories in the path. Salvage each lower directory in turn until you have salvaged the deleted directory that contained the file. You can then search for the deleted file in the salvaged directory.

   - The **Purge all files** option allows you to purge all deleted files on the selected volume.
   - The **Salvage** option allows you to recover a deleted file.
   - The **Purge** option allows you to purge a deleted file.

     You can also select a deleted directory and use this option to purge the deleted directory and all of the deleted subdirectories and files that it contains.

12.2.6 Purging a Deleted NSS Volume

For volume salvage, the NSS volumes are automatically retained on deletion. The deleted volume can be salvaged for a period of time that is determined by the server-level Logical Volume Purge Delay setting. Administrators with the Supervisor right can salvage or purge deleted volumes at any time before the purge delay elapses. For information about the NSS volume salvage feature, see "Volume Salvage versus File Salvage" in the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

1. In OES Remote Manager, select **Manage NCP Services > Manage Shares**.
2. In the right pane, view the list of mounted NSS volumes in the **Active Shares** list.

3 Next to the volume name, click the **Information** icon (I) to go to the volume's Share Information page.

4 Scroll down to the **Volume Tasks** table, then click **Purge Volume**.

12.2.7 Viewing Open File Information for an NSS Volume

1 In OES Remote Manager, select **Manage NCP Services > Manage Shares**.

2 In the right pane, view the list of mounted NSS volumes in the **Active Shares** list.

3 Next to the volume name, click the **Information** icon (I) to go to the volume's Share Information page.

4 Below the **Information** table, click **Open File Information** to open the Open File Information page.

5 View the following information about files on the NSS volume:

- Connection

  For information, see "Managing Connections for NCP Volumes and NSS Volumes" in the *OES 2018 SP3: NCP Server for Linux Administration Guide*.

- User name
- Open file list

12.3 Generating Inventories for Directories or NCP Volumes

With this feature, you can inventory NCP mounted volumes or general file system directories. You can also view graphs, profiles, reports, and key statistics about each of these items, including space usage trends.

Generating this report can take a while, depending on the number of files and folders in the specified directory path.

With a few clicks, you get available space trend graphs; profiles for file types, file owner, last accessed, last modified, creation time, and file size; and links to specific reports for each of these. You can also customize the scan to look for specific file information.

The **File Owner Profile** gathers the ownership statistics from the NSS management interface. If the eDirectory user name is available from the NSS management interface, the file owner is reported as the eDirectory user name, such as `jsmith`. Otherwise, the owner is reported as the `nobody` user. It is not required that you enable the users with Linux User Management (LUM) to get the file owner's name.

NOTE: If AD users are assigned as trustees, then the file owner is reported as the `Unknown` user.

This section includes the following tasks:

- Section 12.3.1, "Generating a File Inventory Report," on page 120
- Section 12.3.2, "Generating an NCP Volume Inventory Report," on page 122
- Section 12.3.3, "Viewing a Saved NCP Inventory Report," on page 124

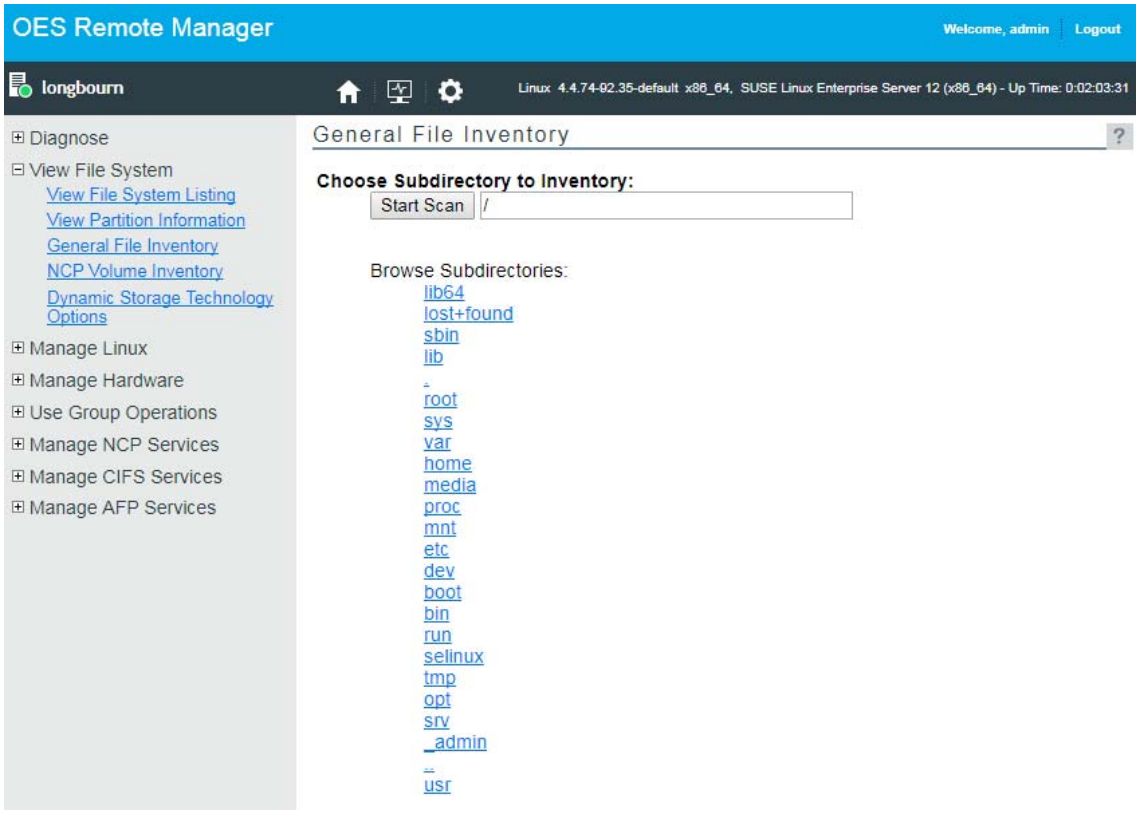
12.3.1 Generating a File Inventory Report

To generate an inventory report for an entire server or any subdirectory, including mounted NCP volumes:

1 Click **View File System > General File System Inventory**.

You can also click the **Inventory** link at the top of the View File System Listing page, and on subsequent pages as you navigate through the file system subdirectories.

This opens the General File Inventory page. By default, the / (`root`) directory is selected.

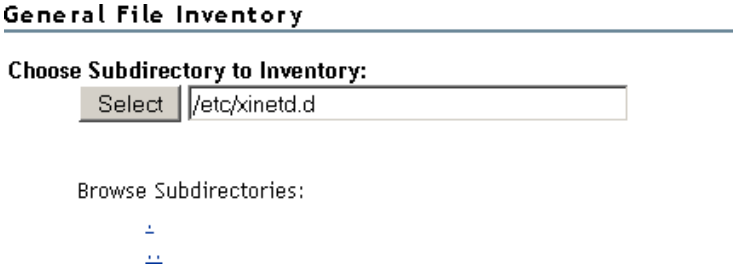


2 From this point, you can do the following:

Click the **Start Scan** button to generate an inventory of the entire server (the default selection is the / [`root`] subdirectory).

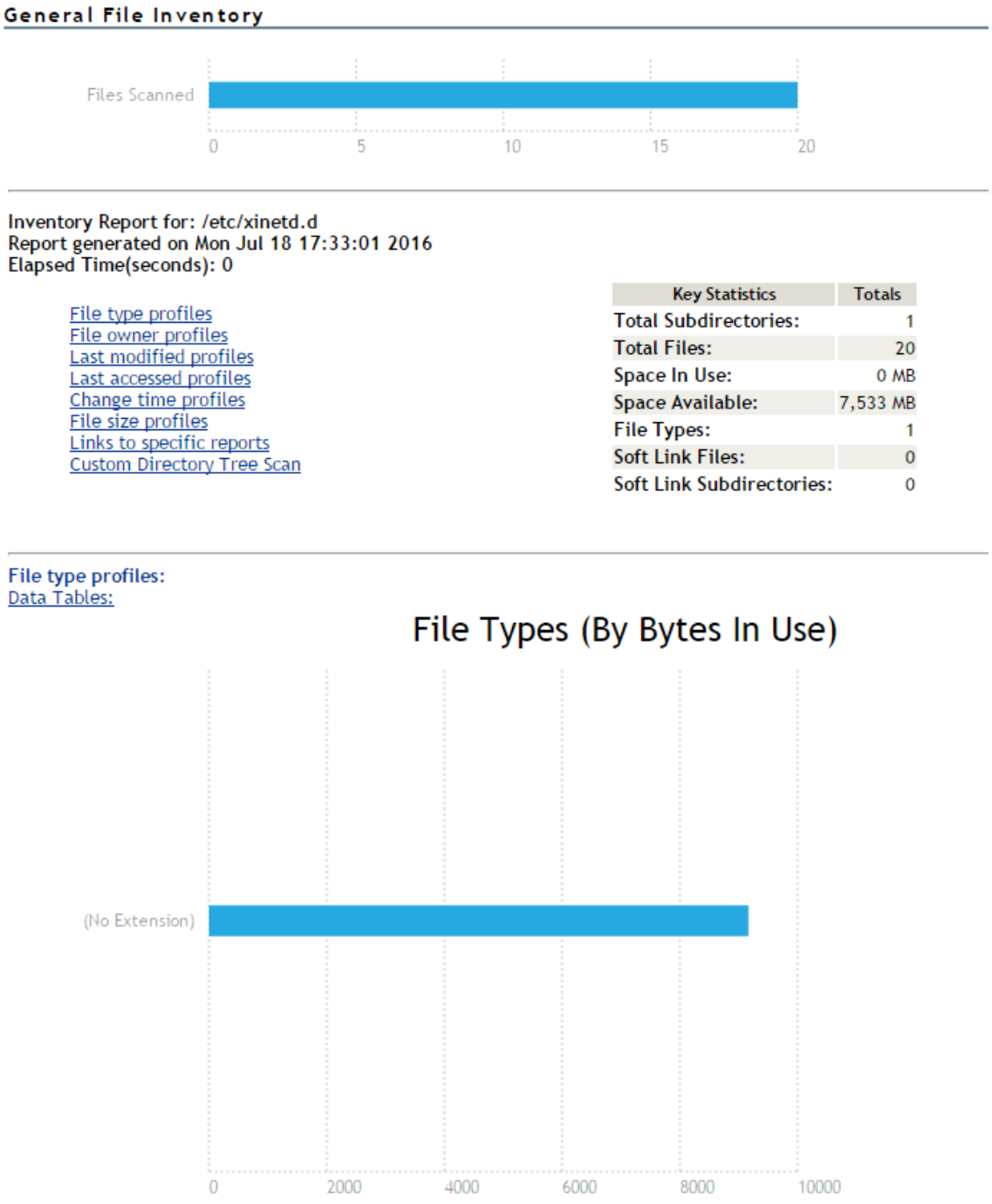
or

Select a subdirectory to generate a report from. Click the *subdirectory_name* links until the desired subdirectory appears in the **Scan** field, then click the **Start Scan** button.



If you are viewing the File System Listing page for the desired directory, you can generate the same reports by clicking the **Inventory** link on this page.

A report similar to the following is generated:

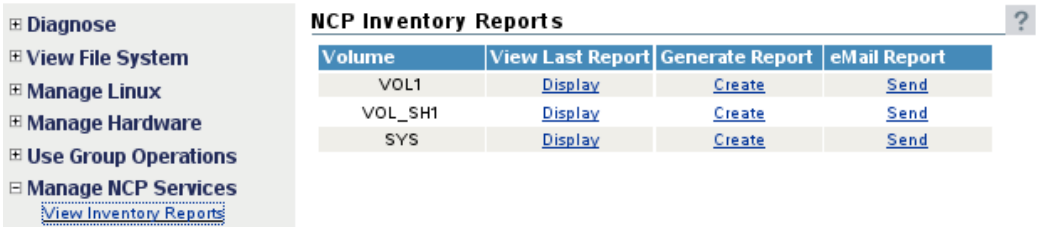


At this point, you can click any of the links to the left of the **Key Statistics** table to move quickly to the generated information, or you can create a custom report. See "Generating a Custom Inventory Report from a File Inventory Report" on page 125.

12.3.2 Generating an NCP Volume Inventory Report

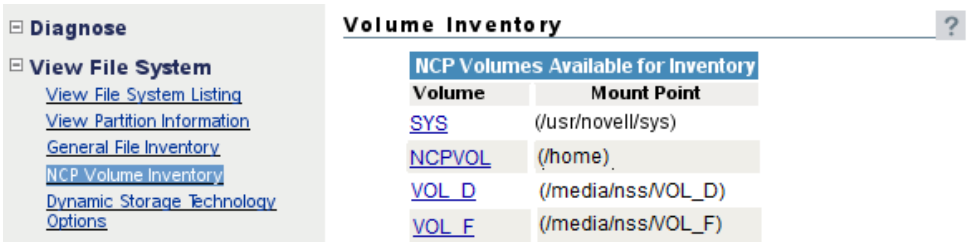
1 Use either of the following methods to generate an NCP Volume Inventory Report:

- Select **Manage NCP Services > Volume Inventory Reports**, locate the NSS volume in the list, then click **Create** in the **Generate Report** column for the volume.



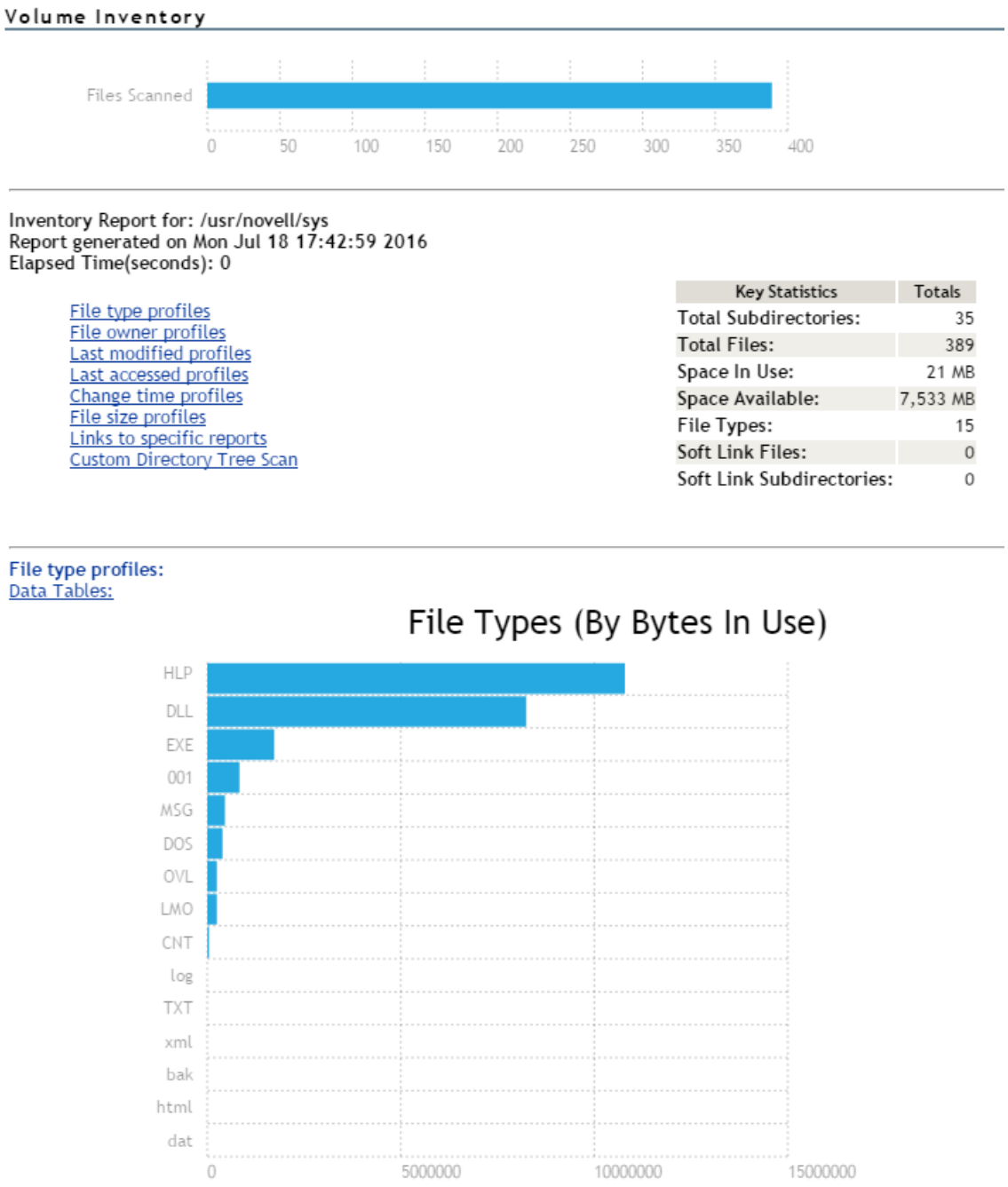
- Select **View File System** > **NCP Volume Inventory**, then select the name link of an available NCP volume in the list.

  This opens the Volume Inventory page that shows all of the mounted NCP and NSS volumes available for inventory.



2 View the generated report.

A report similar to the following is generated:



At this point, you can click any of the links to the left of the **Key Statistics** table to move quickly to the generated information, or you can create a custom report. See "Generating a Custom Inventory Report from a File Inventory Report" on page 125.

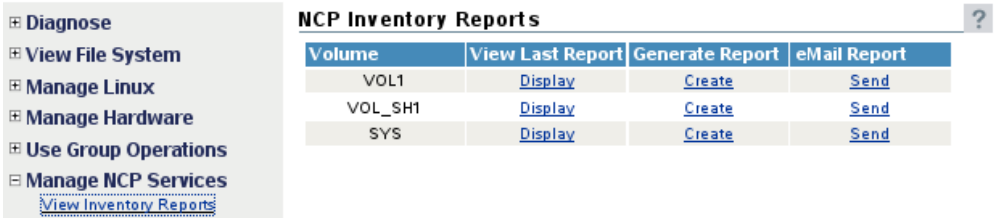
12.3.3 Viewing a Saved NCP Inventory Report

An inventory report is saved when you run an inventory on an NCP volume.

To view the last saved report:

1. Go to the **Manage NCP Services > Volume Inventory Reports** page.
2. Click the **View Last Report > Display** option for the volume.

The saved report provides the same statistics as running **View File Systems > NCP Volumes Inventory**. Graphics are not available in a saved report.



12.4 Generating a Custom Inventory Report from a File Inventory Report

After generating an inventory report for a volume or directory, you can create a customized scan to report more specific information and perform additional actions on the files selected in the report, such as move, copy, or delete.

1 Create the initial report as specified in "Generating a File Inventory Report" on page 120.

2 In the generated report, click the **Custom Directory Tree Scan** link.

A page similar to the following is returned:

3 Type the specific search criteria in the **Search Pattern** field.

. is the default entry.

4 Select the desired settings in the **File Owner Restriction** drop-down box.

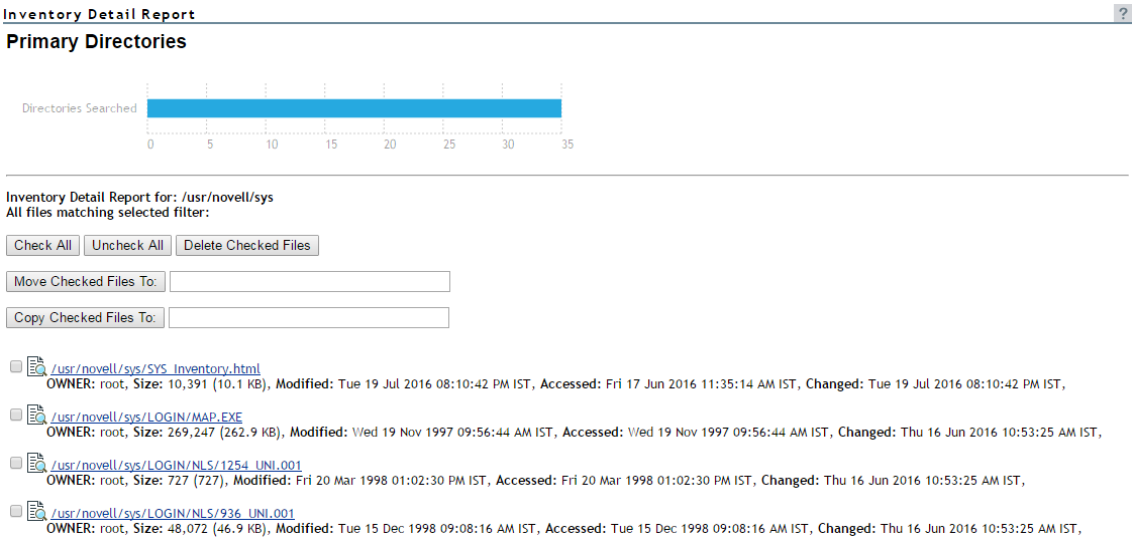
None is the default selection.

5 Select the check boxes desired to customize the report by **Time Stamp** or **File Size** restrictions.

No restrictions is the default setting.

6 Click **Start Scan**.

A page similar to the following is returned:


Inventory Detail Report
Primary Directories
Directories Searched
0 5 10 15 20 25 30 35
Inventory Detail Report for: /usr/novell/sys
All files matching selected filter:
Check All
Uncheck All
Delete Checked Files
Move Checked Files To:
Copy Checked Files To:
/usr/novell/sys/SYS_Inventory.html
OWNER: root, Size: 10,391 (10.1 KB), Modified: Tue 19 Jul 2016 08:10:42 PM IST, Accessed: Fri 17 Jun 2016 11:35:14 AM IST, Changed: Tue 19 Jul 2016 08:10:42 PM IST,
/usr/novell/sys/LOGIN/MAP.EXE
OWNER: root, Size: 269,247 (262.9 KB), Modified: Wed 19 Nov 1997 09:56:44 AM IST, Accessed: Wed 19 Nov 1997 09:56:44 AM IST, Changed: Thu 16 Jun 2016 10:53:25 AM IST,
/usr/novell/sys/LOGIN/NLS/1254_UNI.001
OWNER: root, Size: 727 (727), Modified: Fri 20 Mar 1998 01:02:30 PM IST, Accessed: Fri 20 Mar 1998 01:02:30 PM IST, Changed: Thu 16 Jun 2016 10:53:25 AM IST,
/usr/novell/sys/LOGIN/NLS/936_UNI.001
OWNER: root, Size: 48,072 (46.9 KB), Modified: Tue 15 Dec 1998 09:08:16 AM IST, Accessed: Tue 15 Dec 1998 09:08:16 AM IST, Changed: Thu 16 Jun 2016 10:53:25 AM IST,

12.5 Performing Actions on Files from Custom Reports

After a custom report is generated, you can perform the following actions on the files listed in the report for the selected volume.

- Section 12.5.1, “Moving Selected Files,” on page 126
- Section 12.5.2, “Copying Selected Files,” on page 127
- Section 12.5.3, “Deleting Selected Files,” on page 127
- Section 12.5.4, “Opening or Downloading a File,” on page 127
- Section 12.5.5, “Managing Individual Files,” on page 127

12.5.1 Moving Selected Files

1 From the generated report, select the check box to the left of each file that you want to move. To move all files in the list, click the **Check All** button.

2 Specify the path where you want to move the selected files in the field to the right of the **Move Checked File To** button.

The target path must be to a location on the same volume.

3 Click the **Move Checked File To** button.

12.5.2 Copying Selected Files

1. From the generated report, select the check box to the left of each file that you want to copy. To copy all files in the list, click the **Check All** button.
2. Specify the path where you want to copy the selected files in the field to the right of the **Copy Checked File To** button.

   The target path must be to a location on the same volume.
3. Click the **Copy Checked File To** button.

12.5.3 Deleting Selected Files

1. From the generated report, select the check box to the left of each file that you want to delete. To delete all files in the list, click the **Check All** button.
2. Click the **Delete Checked Files** button.

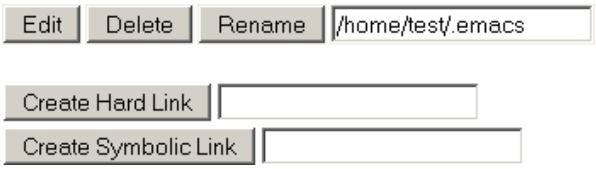
12.5.4 Opening or Downloading a File

1. From the generated report, select the *file_name* link for the file you want to open or download.
2. From the resulting dialog box, select **Open With** or **Save to Disk**, then click **OK**.

12.5.5 Managing Individual Files

1. From the generated report, click the **File Information** icon.
2. To perform the desired action (edit, delete, rename, create hard link, or create symbolic link) for the file, specify the required information in the applicable field, then click the applicable button.

   The target path for the action must be to a location on the same volume.



12.6 Generating and Viewing NCP Trustee Reports for NSS Volumes

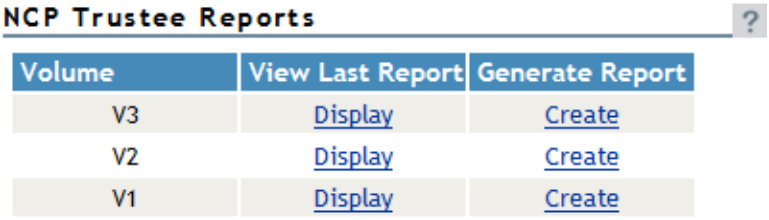
Under **Manage NCP Services**, the **View Trustee Reports** option opens the NCP Trustee Reports page where you can generate a trustee report for a specified NSS volume. This includes Dynamic Storage Technology shadow volumes that are comprised of two NSS volumes. You can display the last trustee report in the web browser. A trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.

In OES 11 SP1 and earlier, you can also send the report to the email addresses that you have pre-configured for OES Remote Manager.

- Section 12.6.1, “Generating an NCP Trustee Report,” on page 128
- Section 12.6.2, “Viewing a Saved NCP Trustee Report,” on page 129

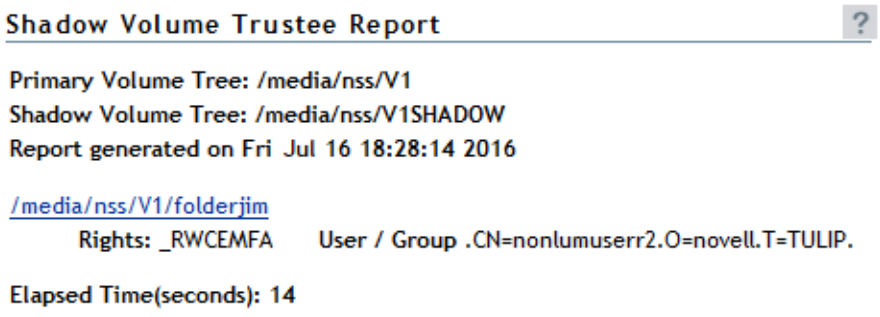
12.6.1 Generating an NCP Trustee Report

1. Log in to OES Remote Manager as the `root` user.
2. In the left navigation panel, select **Manage NCP Services > View Trustee Reports** to open the NCP Trustee Reports page.



3. On the NCP Trustee Reports page, locate the NSS volume in the list, then click its **Create** link in the **Generate Report** column.
4. View the NCP Trustee Report.

   A volume’s trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For example, the following trustee report shows the rights for a folder in a Dynamic Storage Technology shadow volume.


Shadow Volume Trustee Report
Primary Volume Tree: /media/nss/V1
Shadow Volume Tree: /media/nss/V1SHADOW
Report generated on Fri Jul 16 18:28:14 2016
/media/nss/V1/folderjim
Rights: _RWCEMFA User / Group .CN=nonlumuserr2.O=novell.T=TULIP.
Elapsed Time(seconds): 14

12.6.2 Viewing a Saved NCP Trustee Report

You can view the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.

1. Log in to OES Remote Manager as the `root` user.
2. In the left navigation panel, select **Manage NCP Services > View Trustee Reports**.
3. Locate the NSS volume of interest in the list, then click its **Display** link in the **View Last Report** column.

13 Managing Dynamic Storage Technology Options

This section provides an overview of tasks that can be performed when the **NCP Server and Dynamic Storage Technology** plug-in is installed in OES Remote Manager.

For information about using and managing Dynamic Storage Technology on Open Enterprise Server (OES), see the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

For information about using and managing NSS volumes on OES, see the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

The **View File System > Dynamic Storage Technology Options** section in OES Remote Manager for Linux includes the following links to these pages:

Table 13-1 *Links for Dynamic Storage Technology Options*

Link	Actions
View File Systems > Dynamic Storage Technology Options > Volume Information	Volume Share Information ◆ View file system shadow path ◆ Add shadow volume See "Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.
View File Systems > Dynamic Storage Technology Options > Shadow Status	◆ Shadowed ◆ Add Shadow See "Adding a Shadow to the Primary NSS Volume (Linking the NSS Volumes)" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.
View File Systems > Dynamic Storage Technology Options > Inventory	Inventory creates inventory for the primary volume, secondary volume, and merged view of volumes. See "Generating a File Inventory for DST Shadow Volumes" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

Link	Actions
View File Systems > Dynamic Storage Technology Options > Dynamic Storage Technology Policies	• View a list of DST policies. • View summary information about when it was last executed and the total files moved. • Select the policy to view or modify the policy settings. • Select the policy, scroll to the bottom of the Policy page, then click **Delete**. See "Viewing DST Policies and Policy Status" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.
View File Systems > Dynamic Storage Technology Options > Create a new policy	See "Creating and Managing Policies for Shadow Volumes" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.
View File Systems > Dynamic Storage Technology Options > Stop all running policies	See "Stopping a Running Policy" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

View File Systems > Dynamic Storage Technology Options > Duplicate file resolution options	• Broadcast conflict message to user
	• Action to be taken
	  • Show duplicate shadow files (default)
	  • Hide duplicate shadow files
	  • Rename duplicate shadow files
	  • Delete duplicate files from shadow area
	  • Move duplicate shadow files to `/._DUPLICATE_FILES`
	
	See "Resolving Instances of Duplicate Files" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

View File Systems > Dynamic Storage Technology Options > Loading Shadow FS	See "Using ShadowFS to Provide a Merged View for Novell Samba Users" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.
Manage NCP Services > Manage Shares > NCP Shares	NCP Shares • NCP/NSS bindings • Volume Information > Volume Tasks > Add Shadow Volume • Unmount > Volume Information > Volume Tasks > Remove Shadow For information about adding and removing shadow volume pairs, see "Creating and Managing DST Shadow Volumes for NSS Volumes" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

Link	Actions
Manage NCP Services > Manage Server	NCP Manage Server ◆ Global policy parameters for Dynamic Storage Technology DUPLICATE_SHADOW_FILE_ACTION DUPLICATE_SHADOW_FILE_BROADCAST REPLICATE_PRIMARY_TREE_TO_SHADOW SHIFT_ACCESSED_SHADOW_FILES SHIFT_DAYS_SINCE_LAST_ACCESS SHIFT_MODIFIED_SHADOW_FILES For more information about how these settings affect shadow volume pairs on the server, see "Configuring DST Global Policies" in the *OES 2018 SP3: Dynamic Storage Technology Administration Guide*.

14 Managing CIFS Services

The CIFS-NRM plug-in to OES Remote Manager allows you to manage connections and open files on NSS volumes for a CIFS server. When you install Novell CIFS, the plug-in adds the **Manage CIFS Services** section in NRM. With the file monitoring options, you can view details of open files and close open files by connection or by file. The tasks can be performed on NSS volumes where you have configured CIFS shares by using Novell CIFS.

For information about using and managing CIFS services on Open Enterprise Server (OES), see the *OES 2018 SP3: OES CIFS for Linux Administration Guide*.

For information about using and managing NSS volumes on OES, see the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

The **Manage CIFS Services** section includes the following links to CIFS server management pages:

Table 14-1 *Links for Manage CIFS Services*

Link	Page Displayed
Manage Connections	CIFS Connections
View Logs	CIFS System Logs ◆ `libnrm2cifs.log` ◆ `cifs.log`
Manage Open Files	CIFS Open File Management ◆ Connection information (statistics) ◆ Connection listing ◆ Detailed information about a connection, including open files

From these pages you can perform the following tasks:

- Section 14.1, “Managing CIFS Connections,” on page 135
- Section 14.2, “Viewing Log Information,” on page 136
- Section 14.3, “Managing Open Files,” on page 137

14.1 Managing CIFS Connections

By querying or listing all open connections, you can understand how many sessions are opened at any moment. The details for each connection include the session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received. You can drill-down to extract per-connection details, such as the group that the user is a member of.

Table 14-2 *CIFS Connection Parameters*

Parameter	Description
Access mode	Indicates the mode in which the CIFS server has opened the file on behalf of the user. This field displays information that the CIFS server has interpreted from the data received as part of both the Access Mask field and the Share Access field in the SMB_COM_NT_CREATE_ANDX request.
DD	Indicates that the right to delete or rename the file is denied for all other connections.
Desired access	Specifies the access modes that the client has requested.
DR	Indicates that the right to read data from the file is denied.
DW	Indicates that the right to write data into the file is denied.
ND	Indicates that the right to delete or rename the file is denied for this connection.
RD	Indicates that the right to read data from the file is granted.
Shared access	Specifies the sharing modes that the client has requested; that is, how the file should be shared with other users.
WR	Indicates that the right to write data into the file is granted.

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage CIFS Services > Manage Connections** to display the CIFS Connections page.
3. You can perform the following tasks for open connections on a CIFS server:
   - **Status of Open Connections:** The **CIFS Connection List** table displays the connection number, name of user accessing the connection, reads and writes for each connection, CIFS requests by each connection, login details for the connection, and connection type to view CIFS connections for both Active Directory users and eDirectory users.
   - **View Connection Information:** Click the connection name to view more details for a specific connection.

14.2 Viewing Log Information

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage CIFS Services > View Logs** to display the CIFS System Logs page.
3. You can view the following logs for the CIFS server:
   - **libnrm2cifs.log:** Logs debug messages associated with the CIFS-NRM plug-in. Click the file to view the messages.
   - **cifs.log:** Logs information, warning, and error messages associated with the CIFS server. Click the file to view the messages.

14.3 Managing Open Files

You can use the file listing options to view the following information:

- All open files for a particular NSS volume
- All open files by a connection
- All users who have open file handles for a particular file

You can use the file closing options to close the following:

- All open files for a particular NSS volume
- All open files by a particular connection
- All open file handles associated with a particular file

If the user tries to perform any operation on an open file that was closed by using the management tool, the changes might appear the next time the file is opened, depending on the application. However, the data that was saved before the file is closed will be intact.

WARNING: Administrative closure is not the recommended way to close files. It is provided as a tool to administrators to force close files.

---

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage CIFS Services > Manage Open Files** to display the CIFS Open File Management page.
3. The **CIFS Volume** lists the mounted NSS volumes.
4. You can perform the following tasks for files that are open on the selected NSS volume:
   - **Status of Open Files:** The **List of Open Files** table displays the connection number, name of user accessing the file, and path of the file. The files are listed for the selected NSS volume. You can also set a filter for displaying the specific file type for that volume.
   - **Close Files:** Select the files you want to close, then click **Close**. This closes the file immediately and allows no other file operations to be performed. Ensure that you inform the user before closing the file, to allow the user time to save the file; otherwise, the user might lose unsaved data for the file.

15 Managing AFP Services

The AFP-NRM plug-in to OES Remote Manager allows you to manage connections and open files on NSS volumes for AFP server. When you install Novell AFP, the plug-in adds the **Manage AFP Services** section in NRM. You can close connections that are stale and persistent. With the file monitoring options, you can view details of open files and close open files by connection or by file. The tasks can be performed on NSS volumes where you have configured AFP shares by using Novell AFP.

For information about using and managing AFP services on Open Enterprise Server (OES), see the *OES 2018 SP3: OES AFP for Linux Administration Guide*.

For information about using and managing NSS volumes on OES, see the *OES 2018 SP3: NSS File System Administration Guide for Linux*.

The **Manage AFP Services** section includes the following links to AFP server management pages:

Table 15-1 *Links for Manage AFP Services*

Link	Page Displayed
Manage Connections	AFP Connections
View Logs	AFP System Logs ◆ `afptcp.log` ◆ `libnrm2afp.log`
Manage Open Files	AFP Open File Management ◆ Connection information (statistics) ◆ Connection listing ◆ Detailed information about a connection, including open files

From these pages you can perform the following tasks:

- Section 15.1, “Managing AFP Connections,” on page 140
- Section 15.2, “Viewing Log Information,” on page 141
- Section 15.3, “Managing Open Files,” on page 141

15.1 Managing AFP Connections

By querying or listing all open connections, you can understand how many sessions are opened at any moment. The details for each connection include the session ID, client IP address, user name, user login time, consolidated list of read/write requests, access mode, and total number of other requests received. You can drill down to extract per-connection details, such as the group that the user is a member of.

If the connections are stale and persistent (for example, if there is no activity for a considerable amount of time), this session occupies a considerable chunk of memory. In this scenario, the administrator can close the connection/session based on the qualitative analysis of various connection parameters dumped by the new commands/options that are introduced.

Table 15-2 *AFP Connections Parameters*

Parameter	Description
Access mode	Indicates the mode in which the AFP server has opened the file on behalf of the user.
DD	Indicates that the right to delete or rename the file is denied for all other connections.
Desired access	Specifies the access modes that the client has requested.
DR	Indicates that the right to read data from the file is denied.
DW	Indicates that the right to write data into the file is denied.
ND	Indicates that the right to delete or rename the file is denied for this connection.
RD	Indicates that the right to read data from the file is granted.
Shared access	Specifies the sharing modes that the client has requested, that is, how the file should be shared with other users.
WR	Indicates that the right to write data into the file is granted.

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage AFP Services > Manage Connections** to display the AFP Connections page.
3. You can perform the following tasks for open connections on an AFP server:
   - **Status of Open Connections:** The **AFP Connection List** table displays the connection number, name of user accessing the connection, reads and writes for each connection, AFP requests by each connection, and login time details for the connection.
   - **View Connection Information:** Click the connection name to view more details of a specific connection.
   - **Close Connections:** Select the connections you want to close, then click **Close**. This closes the connection immediately, closes its open files, and allows no other file operations to be performed. Ensure that you close any open files before closing the associated connection; otherwise, the user might lose unsaved data for the file.

15.2 Viewing Log Information

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage AFP Services > View Logs** to display the AFP System Logs page.
3. You can view the following logs for an AFP server:
   - **libnrm2afp.log:** Logs debug messages associated with the AFP-NRM plug-in. Click the log file to view the messages.
   - **afptcp.log:** Logs status, debug, and error messages associated with the AFP server. Click the log file to view the messages.

15.3 Managing Open Files

You can use the file listing options to view the following information:

- All open files for a particular NSS volume
- All open files by a connection
- All users who have open file handles for a particular file

You can use the file closing options to close the following:

- All open files for a particular NSS volume
- All open files by a particular connection
- All open file handles associated with a particular file

If the user tries to perform any operation on an open file that was closed by using the management tool, the changes might appear the next time the file is opened, depending on the application. However, the data that was saved before the file is closed will be intact.

WARNING: Administrative closure is not the recommended way to close files. It is provided as a tool to administrators to force close files.

---

1. Log in to OES Remote Manager as the `root` user.
2. Click **Manage AFP Services > Manage Open Files** to display the AFP Open File Management page.
3. You can perform the following tasks for open files on an AFP server:
   - **Status of Open Files:** The **List of Open Files** table displays the connection number, name of the user accessing the file, and path of the file. The files are listed for the selected NSS volume. You can also set a filter for displaying the specific file type for that volume.
   - **Close Files:** Select the files you want to close, then click **Close**. This closes the file immediately and allows no other file operations to be performed. Ensure that you inform the user before closing the file, to allow the user time to save the file; otherwise, the user might lose unsaved data for the file.

16 Tasks Quick Reference

The following table provides information about specific tasks you can perform using OES Remote Manager. These references also link to more specific information in this guide.

Table 16-1 *Task Quick Reference List*

Tasks	Link in Navigation frame or Other Location	For More Information
Build a group for monitoring	**Use Group Operations** > **Configure New Group**	Building and Configuring a Monitoring Group (page 90)
Cron job, schedule	Manage Linux > Schedule Task	"Scheduling cron Jobs to Run on the Server" on page 80
Directory, change attributes of	**View File System** > **View File System Listing**	Viewing Details about Directories and Performing Actions on Them (page 69)
Directory, edit	**View File System** > **View File System Listing**	Viewing Details about Directories and Performing Actions on Them (page 69)
Directory, delete	**View File System** > **View File System Listing**	Viewing Details about Directories and Performing Actions on Them (page 69)
Directory, rename	**View File System** > **View File System Listing**	Viewing Details about Directories and Performing Actions on Them (page 69)
Directory, view detailed information about	**View File System** > **View File System Listing**	Viewing Details about Directories and Performing Actions on Them (page 69)
File, change attributes of	**View File System** > **View File System Listing**	Viewing the Details of a File and Performing Specific Actions (page 71)
File, download	**View File System** > **View File System Listing**	Downloading a File from the Server to a Local Workstation (page 70)
File, edit	**View File System** > **View File System Listing**	Viewing the Details of a File and Performing Specific Actions (page 71)
File, delete	**View File System** > **View File System Listing**	Viewing the Details of a File and Performing Specific Actions (page 71)

Tasks	Link in Navigation frame or Other Location	For More Information
File, rename	**View File System** > **View File System Listing**	Viewing the Details of a File and Performing Specific Actions (page 71)
Files, search for text in	**View File System** > **View File System Listing**	Searching for Text in Files (page 71)
File, upload	**View File System** > **View File System Listing**	Uploading a File to the Server (page 70)
File, view	**View File System** > **View File System Listing**	Viewing Individual Files (page 72)
File system, browse	**View File System** > **View File System Listing**	Browsing File Systems and Performing Actions on Them (page 67)
File system, perform action on	**View File System** > **View File System Listing**	Browsing File Systems and Performing Actions on Them (page 67)
Files, viewing details about	**View File System** > **View File System Listing**	Viewing the Details of a File and Performing Specific Actions (page 71)
Group operations, access an existing group	**Use Group Operations** > **Select Group**	Accessing an Existing Group (page 95)
Group operations, build and configure a new monitoring group	**Use Group Operations** > **Configure New Group**	Building and Configuring a Monitoring Group (page 90)
Group operations, change an existing group	**Use Group Operations** > **Select Group**	Changing an Existing Group (page 95)
Group operations, define or edit Group Monitoring types	**Use Group Operations** > **NRM Health Types**	Defining or Editing Group Monitoring Types (page 98)
Group operations, delete an existing group	**Use Group Operations > Select Group**	Deleting an Existing Group (page 96)
Group operations, discover items to monitor on the network.	**Use Group Operations** > **Configure New Group** > **right-click menu** > **Network Discovery**	Discovering Items on the Network to Monitor (page 99)
Group operations, generate and view server reports	**Use Group Operations** > **Configure New Group** > **right-click menu** > **Save Group**	Generating and Viewing Server Reports (page 96)
Group operations, save a new group	**Use Group Operations** > **Configure New Group** > **right-click menu** > **Save Group**	Saving a Group (page 94)
Group operations, view defined health types	**Use Group Operations** > **NRM Health Types**	Viewing Group Monitoring Types (page 98)
Group operations, view monitored items	**View Monitored Items**	Viewing Monitored Items (page 97)

Tasks	Link in Navigation frame or Other Location	For More Information
Host, shut down	**Manage Linux** > **Down/Reset Options**	Shutting Down and Restarting the Host (page 76)
Host, restart	**Manage Linux** > **Down/Reset Options**	Shutting Down and Restarting the Host (page 76)
Interrupt information, view	**Manage Hardware** > **Interrupt Information**	Viewing Interrupt Information (page 84)
I/O Memory information, view	**Manage Hardware** > **IO Memory Information**	Viewing I/O Memory Information (page 85)
IO Port information, view	**Manage Hardware** > **IO Port Information**	Viewing I/O Port Information (page 86)
Kernel modules, view	**Manage Linux** > **Kernel Module Listing**	Viewing Kernel Modules (page 75)
Mounted devices, perform actions on them	**Home** icon > **Info** icon	Viewing Mounted Devices and Performing Actions on Them (page 66)
Mounted devices, view	**Home** icon > **Info** icon	Viewing Mounted Devices and Performing Actions on Them (page 66)
Packages, install	**Manage Linux** > **Package Information**	Managing Packages (page 77)
Packages, remove	**Manage Linux** > **Package Information**	Managing Packages (page 77)
Packages, view information about	**Manage Linux** > **Package Information**	Managing Packages (page 77)
Partition information, view	**View File System** > **View Partition Information**	Viewing Partition Information (page 72)
Process, kill	**Manage Linux** > **Process Information**	Managing Processes (page 79)
Process, view information about	**Manage Linux** > **Process Information**	Managing Processes (page 79)
Processors, view information about	Manage Hardware > **View Processors**	Viewing Processors (page 83)
OES Server health	**Diagnose > Server Health Values** Diagnose > Server Health Services	Diagnosing Problems Using Ganglia and Nagios (page 39)
OES Nagios	**Configuration Options > Nagios Configuration**	Configuring Nagios (page 47)
OES Nagios user management	**Configuration Options > Nagios Configuration > Nagios User Management**	Managing Nagios Users (page 56)

Tasks	Link in Navigation frame or Other Location	For More Information
OES Nagios alert notification system for Ganglia and Nagios health alerts	**Configuration Options** > **Nagios Configuration**	Modifying the Nagios Notification Methods for Contacts (page 58)
Server Group, monitor overall server health	**Use Group Operation** > **Configure New Group** or **Select Group**	Building and Configuring a Monitoring Group (page 90)
SMBIOS information, view	**Manage Hardware** > **SMBIOS Information**	Viewing SMBIOS Information (page 87)

17 Troubleshooting OES Remote Manager

This section describes known issues and workarounds for OES Remote Manager for Open Enterprise Server.

- Section 17.1, “Daemon httpstkd Is Unable to Start,” on page 147
- Section 17.2, “Error while loading shared libraries: libldapx.so.0,” on page 147
- Section 17.3, “Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2018 or Later,” on page 148
- Section 17.4, “Ganglia Statistical Graphics Are Not Displayed in the Web Browser,” on page 149

17.1 Daemon httpstkd Is Unable to Start

The OES Remote Manager daemon `httpstkd` might be unable to start if the ports it is trying to use are busy. This error is commonly shown by applications when the ports it uses (in this case NRM ports 8008 and 8009) are busy and do not respond. In this situation, you can start `httpstkd` without needing to reboot the server by modifying the ports used by OES Remote Manager in the `/etc/opt/novell/httpstkd.conf` file:

1. Log in to the server as the `root` user.
2. Open the `/etc/opt/novell/httpstkd.conf` file in a text editor.
3. Change the default ports 8008 and 8009 to other unused ports on the following lines:

   ```
   addr 0.0.0.0:8008
   addr 0.0.0.0:8009 keyfile=/etc/opt/novell/httpstkd/server.key
                     certfile=/etc/opt/novell/httpstkd/server.pem
   ```

4. Save your changes, then close the `/etc/opt/novell/httpstkd.conf` file.
5. Open a terminal console, then start the `httpstkd` daemon by entering:

   ```
   rcnovell-httpstkd start
   ```

17.2 Error while loading shared libraries: libldapx.so.0

The following error might occur during the OES Remote Manager installation if eDirectory is not yet available:

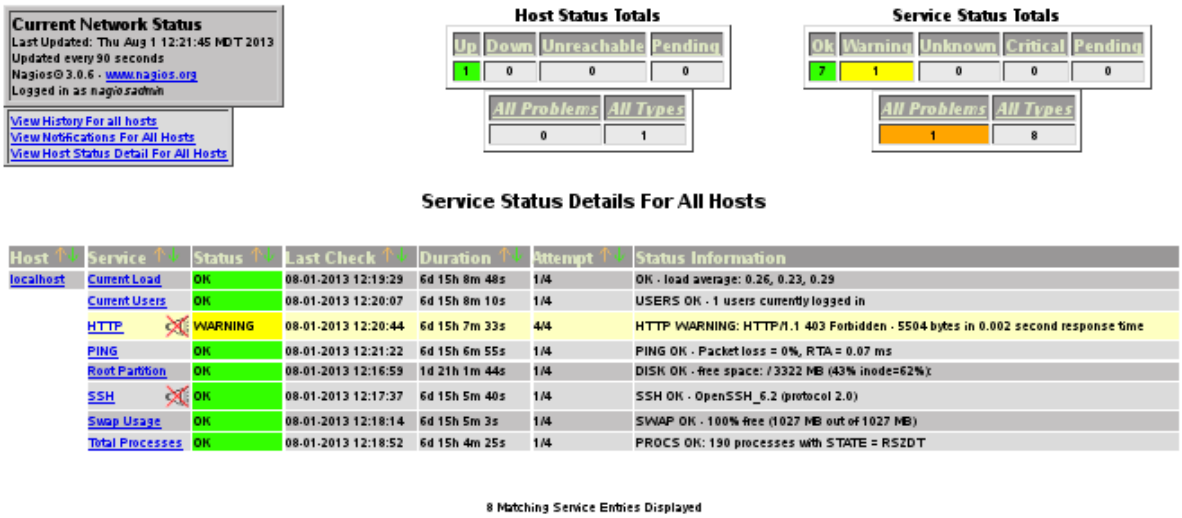
```
Starting the Novell Small Http Interface
Daemon/opt/novell/httpstkd/sbin/httpstkd: error while loading shared
libraries:
libldapx.so.0: cannot open shared object file: No such file or directory
```

Httpstkd tries to start after the rpm is installed. It cannot start at that time if eDirectory has yet to be installed. When you get the `Installation Completed` dialog box, the httpstkd daemon is running.

17.3 Apache 403 Warning Error Reported in Nagios on a New Installation or Upgrade to OES 2018 or Later

You might see an Apache 403 Forbidden Warning error reported in Nagios after a new installation or upgrade to OES 2018 or later.

Figure 17-1 *HTTP 403 Forbidden Warning Error*


Current Network Status
Last Updated: Thu Aug 1 12:21:45 MDT 2013
Updated every 90 seconds
Nagios® 3.0.6 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
1 0 0 0
All Problems All Types
0 1
Service Status Totals
Ok Warning Unknown Critical Pending
7 1 0 0 0
All Problems All Types
1 8
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
localhost Current Load OK 08-01-2013 12:19:29 6d 15h 8m 48s 1/4 OK - load average: 0.26, 0.23, 0.29
Current Users OK 08-01-2013 12:20:07 6d 15h 8m 10s 1/4 USERS OK - 1 users currently logged in
HTTP WARNING 08-01-2013 12:20:44 6d 15h 7m 33s 4/4 HTTP WARNING: HTTP/1.1 403 Forbidden - 5504 bytes in 0.002 second response time
PING OK 08-01-2013 12:21:22 6d 15h 6m 55s 1/4 PING OK - Packet loss = 0%, RTA = 0.07 ms
Root Partition OK 08-01-2013 12:16:59 1d 21h 1m 44s 1/4 DISK OK - free space: / 3322 MB (43% inode=62%):
SSH OK 08-01-2013 12:17:37 6d 15h 5m 40s 1/4 SSH OK - OpenSSH_6.2 (protocol 2.0)
Swap Usage OK 08-01-2013 12:18:14 6d 15h 5m 3s 1/4 SWAP OK - 100% free (1027 MB out of 1027 MB)
Total Processes OK 08-01-2013 12:18:52 6d 15h 4m 25s 1/4 PROCS OK: 190 processes with STATE = RSZDT
8 Matching Service Entries Displayed

To resolve the issue, you can try the following:

1. Log in to the server as the `root` user, open a terminal console, then navigate to the `/etc/nagios/objects` directory.
2. In the `localhost.cfg` file, modify the `check_command` parameters in the section, "# Define a service to check HTTP on the local machine":

   At the command prompt, enter

   ```
   define service {
                   use        local-service    ; Name of service template
   to use
                    host_name              localhost
                    service_description    HTTP
                     check_command         check_http! -e 'HTTP/1.0
   200','HTTP/1.1 200','HTTP/1.1 403 Forbidden'

                     notifications_enabled 0
                 }
   ```

3. Restart Nagios.

   ```
   rcnagios restart
   ```

4. After a few minutes, verify that the HTTP status for Nagios has been updated to the **OK** (green) state.

   4a Log in as the `root` user to OES Remote Manager.

   4b Select **Diagnose > Server Health Services**, then click **Nagios Service Detail**.

4c In the Nagios Authentication Required dialog box, specify your Nagios user credentials, then click **OK**.

4d View the HTTP status in the Nagios main dashboard.

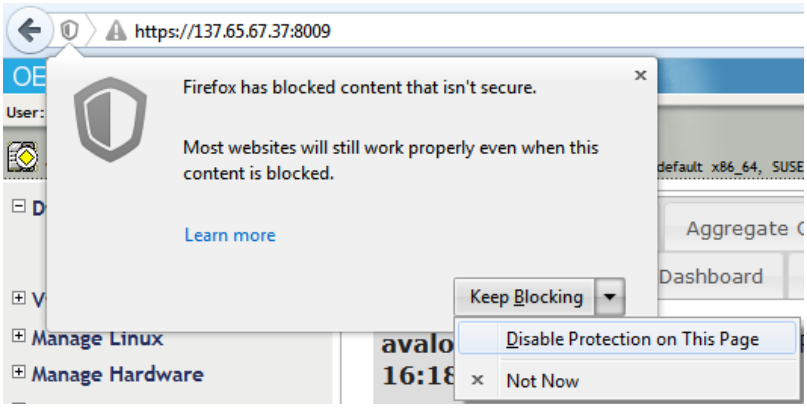
17.4 Ganglia Statistical Graphics Are Not Displayed in the Web Browser

The OES Remote Manager frame sends secure content. However, Ganglia uses scripts to graphically display statistics that send the statistical data via HTTP instead of HTTPS. Depending on how your web browser is configured to handle mixed content on a web page, the Ganglia statistics might not be displayed in the graph windows.

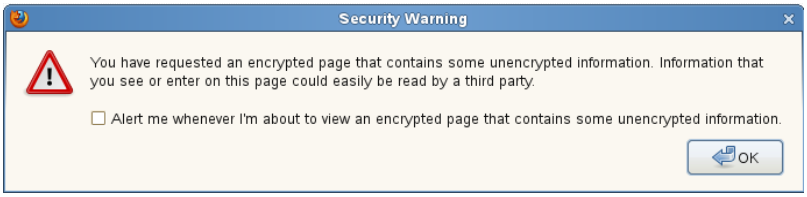
- Section 17.4.1, “Firefox,” on page 149
- Section 17.4.2, “Internet Explorer,” on page 150
- Section 17.4.3, “Chrome,” on page 150

17.4.1 Firefox

In Firefox 23 and later, when you access a page with both HTTPS and HTTP content, a shield icon appears in the address bar, and the browser automatically blocks certain content such as non-secure scripts. To allow mixed content, right-click the shield icon, then select **Disable Protection on This Page**. After you disable protection, an orange alert icon appears in the address bar and makes you aware that the displayed page contains mixed content.



In a Mozilla Firefox 22 and earlier web browser, you receive a warning, but content is not automatically blocked. A **Security Warning** pop-up dialog box reports: `You have requested an encrypted page that contains some unencrypted information`. Click **OK** to dismiss the warning and allow mixed content to be displayed.


Security Warning
You have requested an encrypted page that contains some unencrypted information. Information that you see or enter on this page could easily be read by a third party.
Alert me whenever I'm about to view an encrypted page that contains some unencrypted information.
OK

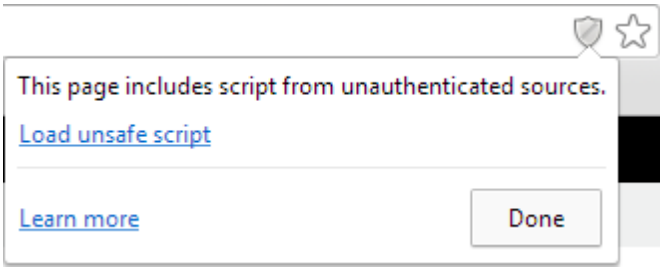
A round shield icon replaces the lock to the left of the https:// in the address bar. Right-click the icon to view the message that advises: `Your connection to this site is only partially encrypted, and does not prevent eavesdropping`.

17.4.2 Internet Explorer

In a Microsoft Internet Explorer web browser, the pop-up dialog box is displayed at the bottom of the page and reports: `Only secure content is displayed`. Click **Show all content** to dismiss the warning and allow mixed content to be displayed.

17.4.3 Chrome

In a Google Chrome web browser, a shield appears at the end of the URL in the address bar. It warns: `This page includes scripts from unauthenticated resources`. Right-click the shield, then click **Load Unsafe Script**.



While mixed content is displayed in Chrome, the green text `https://` and lock in the URL https://, which indicates secure-only content, is automatically changed to red text that is crossed out and a gray lock with a red X https://.

18 Security Considerations

This section contains information that helps you know whether you can use this utility in a secure environment and points you to information to help you set up access to your server so you can be certain that its contents are not compromised through the use of this utility.

For additional security implementation information, see "Security" in the *OES 2018 SP3: Planning and Implementation Guide*.

The default settings for NRM on OES Linux are set so your network and information cannot be compromised. If you change settings from the default, please be aware of the consequences of your actions.

- Section 18.1, "Security Features," on page 151
- Section 18.2, "Security Characteristics," on page 153
- Section 18.3, "Security Configuration," on page 154
- Section 18.4, "Nagios Security Configuration," on page 156

18.1 Security Features

The following table contains the security features of NRM on OES Linux.

Table 18-1 *Security Features of NRM on OES Linux*

Feature	Yes/ No	Details
Users are authenticated	Yes	Users of OES Remote Manager must provide a user name and password credentials to log in. Log in as user `root`, a local Linux user, or as a NetIQ eDirectory user that is Linux User Management enabled. The user sees only those functions that the user has permissions to view or manage. The `root` user is authenticated locally, not through eDirectory. This allows the `root` user to manage server resources even if the eDirectory services are not available. The `root` user has all permissions necessary to manage all functions in OES Remote Manager. For more information, see "Accessing OES Remote Manager" on page 22 and "Changing the HTTPSTKD Configuration" on page 31.

Feature	Yes/ No	Details
Certificate handling by the web browser	Yes	Certificate handling requires SSL 2.0 or later, or TLS 1.0 or later, to be enabled in your web browser. Otherwise, the browser displays an error indicating that the page cannot be displayed. We recommend the higher security options of SSL 3.0, or the latest TLS if it is available.

Limited root user privileges for the Admin user	Yes	User `root` can restrict all users from logging in, so the Admin user or Admin-equivalent user is not granted unlimited root privileges for security reasons. If the server is LUM enabled, the Admin user and users with rights equivalent to the Admin user have the limited `root` user privileges that are needed to modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.
		
		The Admin user or equivalent user needs `root` privileges to modify the following files in order to configure and manage NRM. The privileges are temporary and only for the task to be performed.
		
		`/etc/opt/novell/httpstkd.conf`
		`/etc/pam.d/httpstkd`
		
		The following file names are the names that are used as the description for a specified task:
		
		`/etc/cron.d/[task file name]`
		
		The following files may be the actual file or a symbolic link to the YAST or eDirectory certificates:
		
		`/etc/opt/novell/httpstkd/server.pem`
		`/etc/opt/novell/httpstkd/server.key`
		
		The following files are already modifiable by the Admin user:
		
		The first category has names that are whatever the user names the group that they create.
		`/opt/novell/nrm/NRMGroups/[nrm group names]`
		`/etc/opt/novell/nrmhconfig.conf`
		`/etc/opt/novell/nrmsvchlthcfg.conf`

Servers, devices, and services are authenticated	Yes	When gathering information with group operations, OES Remote Manager authenticates to other servers.

Feature	Yes/ No	Details
Access to information is controlled	Yes	Access to information is restricted to valid users who have rights to access the server through eDirectory or access rights to the local file system. The port for accessing the login dialog box must be open through a firewall if you want the server to be accessible outside the firewall. You can restrict access to specific workstations or a range of IP addresses. For more information, see "Accessing OES Remote Manager" on page 22 and "Changing the HTTPSTKD Configuration" on page 31.
Roles are used to control access	No	OES Remote Manager does not have role-based management.
Logging and security auditing is done	Yes	
Data on the wire are encrypted by default	Yes	The following data are encrypted on the wire: ◆ Administration via browser UI ◆ When logging in the administration is switching to the HTTPS protocol.
Data is stored encrypted	No	
Passwords, keys, and any other authentication materials are stored encrypted	Yes	
Security is on by default	Yes	

18.2 Security Characteristics

OES Remote Manager communicates using port 8008 and 8009. Port 8008 access the Login page, then all other communications take place through secure HTTP ports 8009. These default settings can be changed using options in the `/etc/opt/novell/httpstkd.conf` file.

The HTTPS communication uses SSL encryption. It uses the server certificate by default; however, you can reconfigure this setting if desired.

You can set the SSL key cipher strength by setting the `cipher strength` command in the `/etc/opt/novell/httpstkd.conf` file. We recommend that you set the cipher strength to high, which allows only 112-bit or greater encryption. By default it is set ALL, which allows any cipher strength. For information, see Section A.8, "SSL Key Cipher Strength Command," on page 165.

By default, OES Remote manager sets an HttpOnly cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting. For information, see Section A.4, "HttpOnly Command," on page 161.

The Admin user and users with rights equivalent to user Admin have limited `root` user privileges that are needed to modify only the configuration files necessary for configuring NRM or any other files that NRM has been assigned rights to allow modifying. For a list of these files, see Section 18.1, “Security Features,” on page 151. The user Admin or equivalent user has access according to the Linux and LUM file rights to all other files.

18.3 Security Configuration

The following table provides a summary of the options you can change to allow or limit access to the server through OES Remote Manager.

Table 18-2 *Options for Changing or Limiting Access to a Server Through OES Remote Manager*

Issue/Feature	Recommendation	For More Information
SSL key cipher strength	High (112-bit or greater encryption) The default setting is ALL, which allows any encryption level.	Section A.8, “SSL Key Cipher Strength Command,” on page 165
Let the `root` user access OES Remote Manager with full management rights.	This is the default setting. The root user is the only user with full management rights in OES Remote Manager. By default, only the root user and LUM-enabled eDirectory users can log in to OES Remote Manager. Non-LUM-enabled eDirectory users cannot access the server through OES Remote Manager. We recommend that the `root` user be the only local user created on the system. However, if local users log in to OES Remote Manager, their access is limited to viewing the file systems that they have the local rights to see. The management features are not available to non-`root` local users.	“Accessing OES Remote Manager” on page 22.
Let all LUM-enabled eDirectory users access file system information in OES Remote Manager.	All non-local user access is controlled by eDirectory and LUM. LUM-enabled eDirectory users can log in and view the file systems that they have the eDirectory rights and file system rights to see. These users (including Admin users and Admin-equivalent users) do not have management rights in OES Remote Manager.	“Accessing OES Remote Manager” on page 22.
Deny access to all non-LUM-enabled eDirectory users.	The eDirectory users that are not LUM enabled cannot access the server through OES Remote Manager.	

Issue/Feature	Recommendation	For More Information

Deny access to all LUM-enabled eDirectory users, including the Admin user and Admin-equivalent users.	Set the `nolum` option in the `/etc/opt/novell/httpstkd.conf` file and edit the `/etc/pam.d/httpstkd` file.
	
	Remove these lines:
	
	`auth sufficient pam_nam.so`
	`account sufficient pam_nam.so`
	`password sufficient pam_nam.so`
	`session optional pam_nam.so`
	
	When the `nolum` option is set, no LUM-enabled eDirectory user can access the server via OES Remote Manager, including the Admin user and Admin-equivalent user. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the `root` user has full management access to OES Remote Manager.
		◆ "Changing the HTTPSTKD Configuration" on page 31.
		◆ "Accessing and Editing the HTTPSTKD Configuration File" on page 33.

Restrict access for all LUM-enabled eDirectory users, except the Admin user and users with rights equivalent to Admin. Deny access to all non-LUM-enabled eDirectory users.	Set the `supervisoronly` option in the `/etc/opt/novell/httpstkd.conf` file. When the `supervisoronly` option is set, the Admin user and Admin-equivalent users are the only LUM-enabled eDirectory users that can log in to OES Remote Manager. They can view the file systems that they have the eDirectory rights and file system rights to see. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the `root` user has full management access to OES Remote Manager.	◆ "Changing the HTTPSTKD Configuration" on page 31. ◆ "Accessing and Editing the HTTPSTKD Configuration File" on page 33.
Restrict access to specific workstations or a range of IP address	Set the `filteraddr` and `filtersubnet` options in the `/etc/opt/novell/httpstkd.conf` file.	◆ "Changing the HTTPSTKD Configuration" on page 31. ◆ "Accessing and Editing the HTTPSTKD Configuration File" on page 33.
Remove access to the utility for all users	Stop the HTTPSTKD daemon.	"Starting or Stopping HTTPSTKD" on page 23.

18.4 Nagios Security Configuration

By default, Nagios defines a default user *nagiosadmin* with no password and a default contact *nagiosadmin*. Before you can log in to the Nagios website, you must set a password for the Nagios user `nagiosadmin`. For information about configuring a password and setting up contact information for the Nagios user `nagiosadmin`, see Section 7.5.1, “Configuring Nagios Authenticated Users and Contacts,” on page 47.

A HTTPSTKD Configuration File Options

To control the behavior of OES Remote Manager on Linux, you can specify the options listed in the HTTPSTKD configuration file in `/etc/opt/novell/httpstkd.conf`. This information is in the default configuration file when installing a new server. If you modify the settings, you can view the default file settings in the `/etc/opt/novell/httpstkd.conf.org` file.

If you are upgrading your server, you might need to update or add the information and settings noted if you want the applicable functionality.

To edit the `/etc/opt/novell/httpstkd.conf` file in OES Remote Manager:

1. Log in to OES Remote Manager as the `root` user of the target server.
2. Click the **Configure** icon in the header frame.
3. On the OES Remote Manager Configuration Options page, click **HTTP Interface Management > Edit httpstkd config file**.
4. Modify the settings.
5. To keep the changes, click **Save Changes**.

   The main content frame opens to the **Directory Listing** for the `/etc/opt/novell` folder. You can verify the date and time on the file.
6. Restart the httpstkd daemon to apply the changes.

   6a Click the **Configure** icon to return to the Configuration Options page.

   6b Under **Daemon Restart**, click **Restart httpstkd**.

The following options are available for controlling the behavior of OES Remote Manager on Linux:

- Section A.1, “Address and Port Commands,” on page 157
- Section A.2, “Disable Auto LUM Command,” on page 158
- Section A.3, “Filtering Commands,” on page 160
- Section A.4, “HttpOnly Command,” on page 161
- Section A.5, “InventoryResolveNonLumOwnerName Command,” on page 162
- Section A.6, “Language Commands,” on page 162
- Section A.7, “Load Command,” on page 164
- Section A.8, “SSL Key Cipher Strength Command,” on page 165
- Section A.9, “Supervisor Only Command,” on page 165

A.1 Address and Port Commands

Purpose

Specifies each address and port that HTTPSTKD opens and listens on.

Optionally, you can enable SSL on the port using the `keyfile` and `certfile` parameters. SSL encrypts the login, so that passwords are not sent over the Internet in plain text.

Syntax

`addr ip_address:port_number`

`addr ip_address:port_number keyfile:key_file_path/keyfile_name.key certfile:certificate_file_path/cerfile_name.pem`

Option	Use
IP_address	One of the following: ◆ 0.0.0.0 ◆ The assigned static IP address of the node A DNS name is not allowed.
port	One of the following for public or secure: ◆ 8008 is the default public port ◆ 8009 is the default secure port ◆ any port not in use on the server If you are accessing OES Remote Manager outside a firewall, these ports must be open.
keyfile=<*keyfile_path/keyfile_name.key*>	A `.key` file is the private key used to encrypt SSL-enabled requests. The key corresponds to the public key in the certificate. `/etc/opt/novell/httpstkd/server.key` is the default path and file name on a new server installation.
certfile=<*certificate_path/certfile_name.pem*>	A `.pem` file is a base64 ASCII encoded SSL certificate and its public key. `/etc/opt/novell/httpstkd/server.pem` is the default path and file name on a new server installation.

Examples

```
addr 0.0.0.0:8008
addr 0.0.0.0:8009 keyfile=/etc/opt/novell/httpstkd/server.key certfile=/
etc/opt/novell/httpstkd/server.pem
```

A.2 Disable Auto LUM Command

Purpose

Only the `root` user has full management rights in OES Remote Manager. The root user is a local superuser, and is not an eDirectory user. This allows the server to be managed even if the eDirectory authentication service is down.

Auto LUM lets eDirectory users that are enabled with Linux User Management (LUM) log in to OES Remote Manager by using their eDirectory user names and passwords. For example, you can log in as user Admin or as a user with rights equivalent to Admin rather than logging in as user `root`. When LUM-enabled eDirectory users access OES Remote Manager, they are allowed to view only the file systems that they have the eDirectory rights and file system rights to see.

NOTE: You can use the `supervisoronly` option to restrict access for LUM-enabled eDirectory users to only the Admin user and users with rights equivalent to the Admin user.

By default, the eDirectory users that are not LUM-enabled cannot access the server with OES Remote Manager. They can view their files via NCP, CIFS, or AFP.

We recommend against creating local users other than the `root` user. However, if non-`root` local users access OES Remote Manager, they must log in using the user name and password created on the local system. Only limited functionality is available.They can view only those file systems that they have the local access rights to see. The `nolum` option does not prevent the local-only users from logging in to OES Remote Manager.

Use the `nolum` command to deny access to all LUM-enabled eDirectory users. By default, non-LUM-enabled eDirectory users continue to be denied access. Only the `root` user has full management access to OES Remote Manager.

Syntax

`nolum`

Option	Use
no setting	This is the default setting. To perform all management functions, users must be logged in as user `root`. To view file system information, LUM-enabled eDirectory users can log in with their eDirectory user name and password. Non-LUM-enabled eDirectory users are denied access. To view local file system information only, non-root local users can log in with their locally created user names and passwords. We recommend against creating non-root local users. When the `nolum` command is not specified, HTTPSTKD checks its PAM configuration file at load time and adds the LUM configuration to it if LUM is installed but not already in its configuration.

Option	Use

nolum	To perform all management functions, users must be logged in as user `root`.
	
	LUM-enabled eDirectory users are denied access. Non-LUM-enabled eDirectory users are denied access.
	
	To view local file system information only, non-root local users can log in with their locally created user names and passwords. We recommend against creating non-`root` local users.
	
	IMPORTANT: Setting this option does not disable LUM if it is already part of HTTPSTKD configuration.
	
	You can remove the auto LUM functionality by manually by editing `/etc/pam.d/httpstkd` and removing these lines:
	
	`auth sufficient /lib/security/pam_nam.so`
	`account sufficient /lib/security/pam_nam.so`
	`password sufficient /lib/security/pam_nam.so`
	`session optional /lib/security/pam_nam.so`
	
	Restart the HTTPSTKD daemon to make the changes effective.

Example

`nolum`

A.3 Filtering Commands

Purpose

Blocks access to OES Remote Manager from all addresses except those specified by these `filteraddr` and `filtersubnet` commands.

Syntax

`filteraddr` *`IP_address`*
`filtersubnet` *`IP_address subnet_mask`*

Command	Use
not specified	Allows access from any address. This is the default setting.
filteraddr	Allows access from specific addresses only.
filtersubnet	Allows access from any address on the specified network or subnet.

Examples

The following command allows access only from address 192.168.20.1:

`filteraddr 192.168.20.1`

The following command allows access from only addresses 192.56.56.0 through 192.56.59.255:

```
filteraddr 192.56.56.0 255.255.252.0
```

A.4 HttpOnly Command

Purpose

OES Remote manager sets an HttpOnly cookie attribute that specifies that the cookie is not accessible through a script. This helps mitigate the risk of cross-site scripting.

Syntax

If the HttpOnly flag is included in the HTTP response header, the cookie cannot be accessed through a client side script.

If you modify the setting, you must restart OES Remote Manager.

```
HttpOnly <true|false>
```

Option	Use
true	Include HttpOnly as an attribute in the response header. This is the default setting.
false	Do not include HttpOnly in the response header.

To disable the HttpOnly attribute:

1. Log in to the server as the `root` user, then open a terminal console.
2. Stop the `httpstkd` daemon by entering

   ```
   rcnovell-httpstkd stop
   ```

3. Open the `/etc/opt/novell/httpstkd.conf` file in a text editor.
4. Review the potential security concerns for changing HttpOnly to false.
5. Change the setting from

   ```
   HttpOnly true
   ```

   to

   ```
   HttpOnly false
   ```

6. Save the file and exit the text editor.
7. Start the httpstkd daemon by entering

   ```
   rcnovell-httpstkd start
   ```

Examples

```
HttpOnly true
HttpOnly false
```

A.5 InventoryResolveNonLumOwnerName Command

Purpose

The `InventoryResolveNonLumOwnerName` command is used when you perform an inventory of NSS volumes and the file owner UID is set to the Nobody user. The Nobody user is reported when a file is owned by a NetIQ eDirectory user that is not enabled with Linux User Management (LUM).

Syntax

If you modify the setting, you must restart OES Remote Manager.

```
InventoryResolveNonLumOwnerName <false|true>
```

Option	Use
false	The inventory does not resolve the user IDs of non-LUM-enabled file owners. The owner is reported as the Nobody user. This is the default setting. This provides faster performance for an inventory of files on an NSS volume when eDirectory users are not LUM enabled.
true	The inventory tries to resolve the user IDs of non-LUM-enabled file owners by using NSS APIs. This can result in a major performance impact for the inventory. The more non-LUM-enabled file owners the inventory encounters, the longer it takes to complete the inventory.

Examples

The following example does not resolve the user IDs of file owners that are not LUM enabled. This is the default setting. The non-LUM-enabled owners are reported as the Nobody user.

```
InventoryResolveNonLumOwnerName false
```

The following example resolves the user IDs of file owners that are not LUM enabled to the user name. The more non-LUM-enabled owners encountered, the longer the inventory can take.

```
InventoryResolveNonLumOwnerName true
```

A.6 Language Commands

Purpose

Sets up a mapping of HTTP Accept-Language header tags for Linux locales. These locales determine the languages in which the browser can view content through the OES Remote Manager utility.

To see a list of possible locales on your Linux server, enter the following at a shell prompt:

```
locale -a
```

Syntax

```
lang HTTP_language_string locale_string
```

Command	Use
lang	Use the following settings: ◆ English: en en_US.UTF8 ◆ US English: en-us en_US.UTF8 ◆ Chinese Simplified: zh-cn zh_CN.UTF8 ◆ Chinese Traditional: zh-tw zh_TW.UTF8 ◆ Czech: cs cs_CZ.UTF8 ◆ French: fr fr_FR.UTF ◆ German: de de_DE.UTF8 ◆ Hungarian: hu hu_HU.UTF8 ◆ Italian: it it_IT.UTF8 ◆ Japanese: ja ja_JP.UTF8 ◆ Polish: pl pl_PL.UTF8 ◆ Portuguese-Brazil: pt pt_BR.UTF8 ◆ Russian: ru ru_RU.UTF8 ◆ Spanish: es es_ES.UTF8 ◆ Slovak: sk sk_SK.UTF8 These are the default settings for this release. In this release, OES Remote Manager supports English, Chinese Simplified, Chinese Traditional, Czech, French, German, Hungarian, Italian, Japanese, Polish, Portuguese-Brazil, Russian, Spanish, and Slovak.

Example

The following commands set the browser languages for English, French, Japanese, and Portuguese:

```
lang en     en_US.UTF8
lang en-us  en_US.UTF8
lang zh-cn  zh_CN.UTF8
lang zh-tw  zh_TW.UTF8
lang cs     cs_CZ.UTF8
lang cs-cz  cs_CZ.UTF8
lang fr     fr_FR.UTF8
lang fr-fr  fr_FR.UTF8
lang de     de_DE.UTF8
lang de-de  de_DE.UTF8
lang hu     hu_HU.UTF8
lang hu-hu  hu_HU.UTF8
lang it     it_IT.UTF8
lang it-it  it_IT.UTF8
lang ja     ja_JP.UTF8
lang ja-jp  ja_JP.UTF8
lang pl     pl_PL.UTF8
lang pl-pl  pl_PL.UTF8
lang pt     pt_BR.UTF8
lang pt-BR  pt_BR.UTF8
lang ru     ru_RU.UTF8
lang ru-ru  ru_RU.UTF8
lang es     es_ES.UTF8
lang es-es  es_ES.UTF8
lang sk     sk_SK.UTF8
lang sk-sk  sk_SK.UTF8
```

More Information

If you are upgrading this server and you want to use this option, you need to add these parameters to the `/etc/opt/novell/httpstkd.conf` file for this server.

A.7 Load Command

Purpose

Loads plug-in files used by OES Remote Manager.

Syntax

`load` *`plug-in_file_path/name`*

Option	Use
plug-in_file_path	`/opt/novell/lib/` is the default path for OES Remote Manager plug-in files.
plug-in_file_name	`libnrm.so` is a default plug-in for OES Remote Manager.

Examples

```
load nrm.so
```

```
load /opt/novell/lib/libnrm.so
```

A.8 SSL Key Cipher Strength Command

Purpose

The Cipher command sets the bit strength for the SSL key that is required to access OES Remote Manager. If you modify the setting, you must restart NRM.

Syntax

```
cipher strength
```

Option	Use
all	Allows any negotiated encryption level. This is the default setting.
low	Allows less than 56-bit encryption.
medium	Allows 56-bit up to 112-bit encryption.
high	Allows 112-bit or greater encryption

Example

The following example allows access to OES Remote Manager only with encryption that is 112-bit or greater:

```
cipher high
```

You must restart OES Remote Manager to apply the change.

A.9 Supervisor Only Command

Purpose

Disables access to the server through OES Remote Manager for all users except `root`. If Linux User Management is enabled for OES Remote Manager, eDirectory user Admin and eDirectory users with rights equivalent to user Admin also have access to the server through OES Remote Manager and can perform the same tasks as user `root`.

Syntax

```
supervisoronly
```

Option	Use
no setting	This is the default setting. Local users and all LUM-enabled eDirectory users can log in to OES Remote Manager. The non-root and non-admin users have limited access to the server through OES Remote Manager. They can access only the server's file systems that they have rights to and can perform very limited tasks such as file upload and text search.
supervisoronly	Lets only user `root` and eDirectory user Admin and users with rights equivalent to Admin have access to the server through OES Remote Manager. LUM must be set for eDirectory user access.

Example

```
supervisoronly
```

More Information

If you are upgrading this server and you want to use this option, you need to add these parameters to the `/etc/opt/novell/httpstkd.conf` file for this server.

B OES Remote Manager Packages

Table B-1 lists the packages that are installed when the OES Remote Manager (NRM) pattern is installed on an Open Enterprise Server (OES) server.

Table B-1 *Packages Contained in the OES Remote Manager Pattern*

Package (RPM)	Description
`novell-lum-providers`	A set of CIM providers to facilitate the management of Linux User Management, which is a plug-in to PAM.
`novell-nrm`	OES Remote Manager, web-based Linux machine management, and control interface. It contains all the binaries and necessary components for OES Remote Manager.

Table B-2 lists the plug-in software that adds functionality to NRM when the related OES Services pattern is installed:

Table B-2 *Packages for Program Plug-Ins to NRM*

RPM	Description
`novell-ncpserv-nrm`	NRM plug-in for the NCP Server and Dynamic Storage Technology
`novell-cifs-nrm`	NRM plug-in for CIFS Services
`novell-afp-nrm`	NRM plug-in for AFP Services

Table B-3 lists the software that NRM depends on to report server and services health information in OES:

Table B-3 *Open Source Packages Used for Server and Services Health Monitoring in OES*

RPM	Description
`novell-ganglia-monitor-core-gmetad`	Ganglia Meta daemon that gathers the health statistics about the server
`novell-ganglia-monitor-core-gmond`	Ganglia Monitor daemon that provides the Ganglia monitoring service
`novell-ganglia-web`	Ganglia Distributed Monitoring System that provides historical graphs of the collected system metrics
`monitoring-plugins-nagios`	Checks the status of the Nagios process on the local machine. It also ensures the Nagios status log is no older than the number of minutes specified by the expires option.
`microfocus-nagios`	Core programs for the Nagios Network Monitor
`microfocus-nagios-www-dch`	The HTML files that do not "call home" and also allow to run the web interface without PHP support
`microfocus-nagios-www`	The HTML and CGI files for the Nagios web interface